



**ANGELA B. COREY**  
STATE ATTORNEY

July 11, 2013

Dear Mr. Kruidbos:

It has come to our attention that you violated numerous State Attorney's Office (SAO) policies and procedures and have engaged in deliberate misconduct that is especially egregious in light of your position as Director of Information Technology (IT).

On March 18<sup>th</sup>, 2013 it was discovered that several SAO computers had been compromised and confidential information had been viewed and copied from a number of "F-drives". Among other things, this hacking involved access to sensitive employee disciplinary matters and personal health information. During the investigation of that serious breach of security you were asked to produce former director, Wes White's, (White) cell phone, ipad and laptop computer. As the SAO IT Director you were tasked with keeping a current inventory and tracking assigned locations of computer equipment. You were also responsible for retrieving office computers and cell phones from employees when their employment with the SAO ended.

You produced several cell phones that you represented as having been assigned to White, when in fact they were not. Only upon repeated requests that you produce White's cell phone did you "discover" that you had 'inadvertently' put that phone in the computer 'server' closet in the Nassau County office. When you finally produced that phone it had been taken back to factory settings, unlike the first two phones that you produced.

During that same investigation it was also discovered that you had re-imaged White's laptop and had deleted public records information that was on that computer. You were specifically instructed by Ms. Corey that destruction of public records was absolutely prohibited and that in the future you were to ensure that all information on any office computer was to be saved before any re-imaging occurred. This instruction was simple, direct and not subject to any misinterpretation.

On March 27, 2013 you were questioned by four directors of the SAO about your involvement in the unauthorized access of various SAO computers. You were told that you were one of only two people who were deemed responsible for copying information

off F-drives without permission to do so. It became a concern at the time that pending case information throughout the office may have been compromised. You were informed of this fear.

After that investigation your duties were significantly changed. On April 3, 2013 you met with Summer Sonson, Jackie Bevel and Cheryl Peek who explained the changes in your employment with the SAO. Among other things, your access to individual F-drives was taken away, you were required to get prior approval from a managing director for any requests that were to be made to the City's IT department, you were to report to the SAO fiscal director for all purchasing and budget matters and you were to get prior written approval of all IT purchases.

Furthermore, your supervisory duties were significantly diminished. Eight employees were removed from your direct oversight. You were left with supervisory responsibility of just two employees. You were also told that your work hours were modified and that you no longer were allowed to take thirty minute lunch breaks in order to shorten your work day. Instead of reporting to work at 8:30 and leaving at 5:00, you were to report to work at 8:00 and work until at least 5:00. You were also told to produce a written job description of your duties and to create a written list of projects on which you were working. You were tasked with giving a written status report on those projects to a managing director.

You were reminded that you must document (in writing) whenever computer equipment was moved or reassigned and you were to immediately inventory all computers belonging to the SAO. Furthermore, the business office was to assume control of inventory of all computer equipment of any individual who was terminated as an employee of the SAO. You were also instructed that when any individual terminated employment with the office, the employee's computer contents were to be saved to a disk. Two copies of the disk were to be given to Ms. Bevel so that she could both preserve the information on the disk and so that she could ensure that the correct supervisor received a copy of the State work product taken from the computer.

You called in to work sick the very next day.

On May 28, 2013 White appeared in court and testified in a hearing in the Trayvon Martin homicide case. White testified that he received information from you about that case and he proceeded to give that information to the defense attorney in that case "5 weeks ago". Pursuant to White's testimony, it would have been on or about April 22, 2013 that he delivered SAO information to the defense team. This was less than three weeks after your duties had been significantly modified. All of this was done without informing any assistant state attorney (or the State Attorney herself) of your complicity with the defense in the pending criminal case.

Since you were placed under subpoena (at the request of White) as a witness in the hearing, there was no choice other than to immediately place you on paid administrative leave.

On June 6, 2013, under oath, you testified that in the course of your duties as the

IT Director for the SAO, you were requested by Bernie de la Rionda to print a Florida Department of Law Enforcement (FDLE) report regarding a cellphone belonging to Trayvon Martin. You were not given this information to do any analysis, create any report or to become an expert witness in the case. In fact, you have never been qualified as an expert on computer issues of any sort in any court of law. As you acknowledged in court on June 6 you are not a forensic expert in this, or any other, area of computer science. FDLE was responsible for all expert analysis and testimony in the homicide case.

In the course of your very limited involvement in the criminal case, you noted that there may be more information available on the cell phone that needed to be explored. You acknowledged that Mr. de la Rionda told you he would turn that information over to the FDLE expert inasmuch as the FDLE expert was the one who would be testifying at trial. Mr. de la Rionda also told you that the source file for the victim's cell phone would be given to the defense in the discovery process. It is indisputable that you were told and understood that both these actions were being taken.

You also knew that the victim's cell phone was taken to Cellebrite in New Jersey via the FDLE expert. You verified that did not know, and did not ask, that the defense team had a chance to go to Cellebrite at the same time and question the Cellebrite experts about the contents of the phone.

You were aware that Mr. de la Rionda provided the cell phone's original source file to the defense and you also knew that the defense had their own IT expert to review the evidence. While you did not know what actions their expert may have done on the case, you were aware that the defense uncovered text messages that even you had not detected.

You apparently (without the courtesy of inquiring further of Mr. de la Rionda) questioned the ethics of an attorney who has been an Assistant State Attorney in the Fourth Judicial Circuit since 1983. He has been a member of the Homicide Unit since 1986 and has previously been a director of the Homicide Division, Circuit Court, and Repeat Offender Court. Mr. de la Rionda won the State Attorney's Office First Annual Distinguished Service Award in 1991 and the Annual Jury Trial Award in 1993. Mr. de la Rionda has tried over 250 jury trials, including 68 murder cases. He has received numerous awards and recognition for his selfless work for over thirty years. His record as an honorable and respected attorney is unblemished and beyond reproach.

Responding to discovery is not within your purview. As you acknowledged, "I don't forward any discovery to attorneys". You are not an attorney and you have never been trained nor authorized to respond to discovery.

You, an individual who is not educated in law or the Rules of Criminal Discovery, considered that Mr. de la Rionda's "approach" in responding to discovery was "inaccurate". Without full knowledge of his actions in this case (because you never sought any clarification) you questioned whether what he did was "correct". You never approached either of the other two seasoned attorneys assigned to the prosecution team, or the State Attorney, to question what had been done.

You had an open door to the State Attorney. You exercised that privilege numerous times over the past four years. You did so as recently as March and April, 2013 during the investigation of the SAO computer security breach and the determination that your oversight of the office technology was abysmal.

You did not pose any questions to any member of the highly experienced trial team or to any of the over 100 attorneys in the office. Neither did you go to any agency or body that had the authority to investigate, police, manage or otherwise remedy any actions you claimed concerned you. Instead, you purloined confidential work product from a pending high profile criminal prosecution (known as the Trayvon Martin case) and surreptitiously sneaked it to an attorney who you stated you "suspected had an axe to grind". As you told the defense attorney at the June 6<sup>th</sup> hearing, you were aware of a recent parting email that White sent to all SAO employees wherein he was clearly "not happy".

After you were put on leave on the morning of May 28, a computer assigned to you was found in the area outside of your office. Typically this computer was either at your home or in your office. It was still powered on but was set back to its original factory settings. Forensic review of that computer revealed that all existing data on the computer was deleted on Friday May 24 at 3:11 pm. That timing is particularly significant inasmuch as on Thursday, May 23 at 5:01 pm and 5:03 pm Jackie Barnard attempted to contact you about information that was being publicized by the defense in the Trayvon Martin case. When you returned her call at 5:34 pm you told her that you left early that day for a doctor appointment. (In contrast to that assertion, the timesheet that you submitted for that date showed that you worked an eight hour day and did not leave until 5:00pm).

Ms. Barnard told you that there was an issue with the victim's "phone download" in the Martin case. She told you that you needed "to call Bernie". You talked to Mr. de la Rionda on Friday May 24 during the mid-morning hours. You acknowledged that you missed some data that the defense had discovered because you did not open the "DB" link. Within less than 24 hours of the defense counsel's publication of the victim's cellphone information, you deleted all information on your office laptop. Monday May 27 was a holiday and the office was closed. On the morning of Tuesday May 28 Wes White took the stand for the defense and announced that you had supplied work product information (including information regarding the victim's cellphone which the court had ruled was exempt from disclosure) to White. White then supplied it to the defense.

Wiping your laptop clean is in direct contradiction to a clear, unequivocal and specific order that was recently reiterated to you that all computer data was to be preserved to comply with Public Records Law. You, the very person who was tasked with preserving electronic public records, were the very one who violated this law.

All these actions show that your intent was not pursuant to any pure motive or genuine concern. Your feigned and spurious claim of possible liability was nothing more than shameful manipulation in a shallow, but obvious, attempt to cloak yourself in

the protection of the whistleblower law. You were not concerned about any possible civil or criminal liability. You never needed to reveal any specific case information to any unauthorized individuals. You needed only ask any one of numerous legitimate agencies or individuals who were available to you if a computer support employee could be at risk for an attorney failing to properly respond to discovery. Your motive in going to your friend, who you thought "had an axe to grind", was out of your own personal dissatisfaction with your recently changed job duties and the fact that you would now have to report to someone who you did not like.

Your actions are professionally reprehensible and violated the written Code of Conduct for the SAO. The Code of Conduct is found both in the Office Manual and the Employee Information Guide. Both documents include instruction to all employees regarding confidential information:

"Confidential Information – Be scrupulous in your use of official information. Ensure that you know about and satisfy the SAO's confidentiality provisions."

Also under examples of grounds for corrective action are the following prohibited activities:

"Disclosure of confidential information",  
"Sabotage of office property or equipment", and  
"Misuse of State Attorney Equipment"

The Manual and the Information Guide also warn that "insubordination, which is defined as a deliberate refusal to follow appropriate orders" can lead to dismissal. Your actions in deleting information on your computer and taking it back to its factory settings without following specific office protocol is insubordination.

On June 6, 2013, under oath, you acknowledged that the work carried on in the SAO is confidential. You further acknowledged that prosecution handled by this Office includes homicides, major crimes, gang activity and other highly sensitive cases and information. You know that case outcomes can be compromised and people's lives can be at risk if information is leaked.

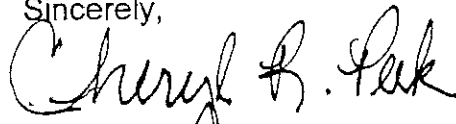
Being the Director of the IT function for the SAO is a position of trust. Your computer background and training give you unfettered access to every computer in the SAO should you ever return. Your egregious lack of regard for the sensitive nature of the information handled by this office is completely abhorrent. You have proven to be completely untrustworthy. Because of your deliberate, wilful and unscrupulous actions, you can never again be trusted to step foot in this office. You have left us with no choice but to terminate your employment.

Your last day of employment is July 11, 2013.

Information regarding COBRA can be found at [www.myflorida.com/mybenefits](http://www.myflorida.com/mybenefits) or by calling People First at 866-663-4735.

For information regarding your pension, please contact FRS directly at 866-446-9377. Your options will depend upon whether you are enrolled in the pension or investment plan and whether or not you are vested.

Sincerely,

A handwritten signature in black ink that reads "Cheryl R. Peek". The signature is written in a cursive style with a large initial "C".

Cheryl R. Peek  
Managing Director  
State Attorney's Office  
Fourth Judicial Circuit