



U.S. Department of Justice

United States Marshals Service

November 26, 2014

Mr. John Young
Attorney, U.S. Office of Special Counsel
1730 M St., NW Ste 300
Washington, D.C. 20036
(202)254-3625

Sir,

After having reviewed the report, I find the lack of acceptance of responsibility and a complete lack of accountability for our people's personal and private data by then AD William Snelson and DAD Angel Gonzales who were the United States Marshals Services (USMS) Investigative Operations Division's senior leadership at the time of the incident incredibly disappointing.

Both Mr. Snelson and Mr. Gonzales receive annual training as it relates to both ethics and the protection of Personally Identifiable Information (PII). They had daily access to the shared drive and it is impossible to believe that they did not see the files or even the folder names which are very telling in themselves. These files contained nearly 7000 unsecured pieces of PII. These ranged from names and social security numbers, to credit cards numbers, grievance files, medical information, disciplinary actions, as well as other significant pieces of PII.

To make matters worse, Mr. Snelson had previously managed the USMS Office of Inspection (USMS Internal Affairs) and the Tactical Operations Division and is well aware of the importance and legal requirements of safeguarding this critical information.

This information impacts USMS operational personnel, contractor's, USMS administrative personnel, as well as, our state, local and federal task force officers.

To be clear the following is *only some* of the information that was compromised:

- *Deputy United States Marshals and administrative employees names, dates of birth, home addresses and social security numbers
- *Deputy United States Marshal's disciplinary files
- *Deputy United States Marshal's grievance files
- *Deputy United States Marshal's medical files and family member's names and addresses
- *State, Local and Federal Task Force Officer's names and social security numbers
- *Government travel and purchase card numbers
- *Significant other potentially damaging PII Information

Again, based on Marshals Thompson's investigation there were nearly *seven thousand failures* to secure both our personnel's and our state, local and federal law enforcement partners Personal

Identifiable Information (PII).

It appears that they began making modifications to the shared drive as soon as they were notified of the breach. Since this investigation involves a violation of law; I would ask was a copy of the shared drive memorialized prior to making any changes to it in order to preserve the evidence in the event of a follow on criminal investigation.

The report claims that they can find no inappropriate use of the financial information. This may be true but it does not mean that it has not happened. They have not shown any way of tracking the access or whether the data was recorded or used by anyone. To my knowledge no mass email has gone out to any past or current USMS employee or task force officer to ask whether their personal information had been compromised or whether their identity was stolen. Anyone could have digitally copied the information, taken a picture of it, printed it or simply written it down for future use.

More importantly no one was notified that their information was compromised or what type of information it was.

Additionally, many of the other inappropriately secured files were of a very personal nature and it is impossible to believe that viewing career selection lists, grievance files, medical files as well as the discipline files of our employees could not have adversely and inappropriately affected peer and leadership's view of those employees. This could have had an impact on their selection for important assignments or even selection for advancement within the agency.

I have personal experience with Mr. Snelson's inappropriate use of personal information to undermine reputations and careers within the agency and have recently learned that he is currently under scrutiny for the inappropriate release of Critical Incident information (PII) which is both wildly inappropriate and may have undermined other careers in the USMS. This occurred while he was the Assistant Director of the USMS Tactical Operations Division.

Additionally, some of the information that I understand was not secured properly was PII data related to two Deputy United States Marshals that were killed in the line of duty. If true, I believe the mismanagement of this information is inexcusable. There, also, appears to be some questions as to his candor in this investigation. I am personally aware of what I believe to be his lack of candor and care for his employees.

I noticed that there was a memo to the USMS Deputy Director Harlow requesting access to both my computer access and my email access. I, however, did not notice the request for the activity logs and e-mails of any other IOD employees to include the Mr. Snelson and Mr. Gonzales. In my opinion it would seem reasonable based on their knowledge of DOJ policy and CSAT Training to determine how many times they had accessed the IOD's shared drive. Would this not show repeated access to the shared drive and dispel the attempt to lay the responsibility on a retired administrative employee. It was their command and their employee's care is their responsibility both morally and legally.

Mr. Gonzales reports a 99% plus record of completion of Computer Security Awareness Training. This means that every IOD employee understands what PII is and how it must be secured. In my opinion, this only makes the issue before us more serious.

The bigger question is why is it that no one, prior to me, brought this up to through the IOD chain of command? How is it that hundreds of highly trained operational and administrative employees can ignore files and folders titled with what are clearly PII violations on a daily basis and not mention or report them?

The answer is sadly simple: FEAR.

Positions, assignments and other cherry perks within IOD are more often handed out based on popularity and cronyism than on merit and bringing sensitive problems that could embarrass the division or the agency leadership is a quick way to become unpopular and eliminated from the club. I can say from what I have seen occur to others over my nearly 19 years with the USMS and from my personal experience it is incredibly safer and more career enhancing to simply look the other way. Additionally, IOD senior leadership has no respect for outside investigations because they have never seen any significant change despite the findings of the investigations. I believe that this actually encourages additional violations of policy.

The agency has claimed to have eliminated access to the files now and for the future, but once again I ask; have they taken the time to notify those compromised that their personal, professional, medical and disciplinary information has been compromised? Does the division/agency not have a responsibility to do so? To notify every administrative, operational employee and every state, local and federal task force officer that their PII was compromised and not secured by the USMS IOD's Leadership?

Isn't that a normal and nearly immediate protocol to care for and protect those who have been compromised?

I understand that USMS OI doesn't have any record of misuse of PII related to the breach but that can in no way represent the potential breach to those whose information was compromised. Without formally notifying all of them how can we find out if their information was misused or not. If a TFO or DUSM in CA, Utah, Texas, far from USMS HQs, had his identity stolen why on earth would he report it to USMS IOD Headquarters or USMS OI; particularly when they have not been provided any information to make that link.

Don't we have both a responsibility and obligation to make that notification? Shouldn't that have been done more than six months ago? Isn't that what we would want if our information had been compromised? Is there a single person that wouldn't demand to know if their information had been compromised by their bank or Credit Card Company?

AD Snelson has shown a pattern of failure as it relates to protecting and securing sensitive equipment (He was the AD for the TOD when the loss of thousands of radios was reported in the Washington Post.) and information while holding senior management positions in the agencies leadership. He has also, shown a pattern of inappropriate treatment for those attempting to disclose violations of policy, law and ethics that could possibly impact him directly.

Additionally, when I attempted to disclose and discuss numerous violations of ethics, law and policy that I know to have occurred I was told by Mr. Snelson amongst other things to:

BE QUIET

This occurred at a meeting with Mr. Snelson on February 21, 2013 at the USMS SERFTF. I have repeatedly disclosed this to senior leadership within our agency all the way up to the Associate Director of Operations (ADO) and Administration (ADA) but no one has pursued it further.

Additionally, when I attempted to report serious violations of use of force, USMS and DOJ policy, as well as, ethics violations I have been urged to be quiet. Following my being reassigned to the OFC, I was met with threats by IOD leadership, as well as, having multiple members of IOD's senior leadership tell me to lay low and stay away from Headquarters (i.e. Mr. Snelson), as well as by Chief Inspector John Smith admonishing me for not being quiet enough with respect to attempting to report the violations.

While the utter failure to secure PII by IOD's leadership is serious problem the underlying issue of leadership who drive their personnel to silence through fear is to me a much more frightening one. It is interesting to see that those who have either looked the other way or actively participated in the silencing of their employees have received significant rewards; i.e. been promoted, received career extensions or were lateralled into better positions under Mr. Snelson.

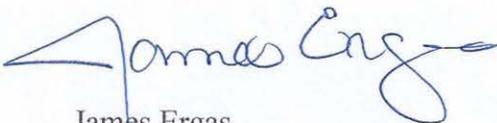
In support of my belief that solving the problem isn't the true goal for either Mr. Gonzales or Mr. Snelson; I find it interesting that I have not even been instructed with what to do with the PII data that I had when I made the complaint. Based on my experience with this leadership the reason is simple. Their response is not to truly solve the problem, take responsibility for the failure, identify and punish those responsible or address the underlying fear of USMS employees to report these violations. The report has been completed in a manner, with the hope, that it will be enough to simply make the problem go away for the agency, specifically for Mr. Snelson and Mr. Gonzales.

I believe that our Director Stacia Hylton and Deputy Director David Harlow have been shielded from the facts of numerous investigations and incidents by the current ADO; William Snelson. I believe this and numerous other issues, violations of policy and law have been hidden or misrepresented by Mr. Snelson to our Director and Deputy Director to ensure and further his career aspirations.

I appreciate your time, the opportunity to address the report, and ask you, my Director and Deputy Director to take a deep look into Mr. Snelson's current and past actions I do not think they will be honored by what they find. I believe that the United States Marshals Service's mantra; Justice, Integrity and Service are more than just words to both of them.

If you have any questions or need any additional information, I am at your service.

Very respectfully,

A handwritten signature in blue ink that reads "James Ergas". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

James Ergas
Chief Inspector
United States Marshals Service