



U.S. Department of Justice

Office of the Deputy Attorney General

Associate Deputy Attorney General

Washington, D.C. 20530

August 22, 2014

The Honorable Carolyn N. Lerner
Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW – Suite 300
Washington, DC 20036-4505

Re: OSC File No. D1-14-1514

Dear Ms. Lerner:

This is in response to your letter of April 23, 2014, regarding a whistleblower disclosure that employees of the U.S. Marshals Service (USMS), Investigative Operations Division (IOD), engaged in conduct that may constitute a violation of law, rule, or regulation. Specifically, USMS Chief Inspector James Ergas alleged that IOD employees failed to follow appropriate procedures for safeguarding and disposing of Personally Identifiable Information (PII) and protected health information on the component's shared hard drive in violation of the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, and Department of Justice policies and procedures.

At the direction of the Attorney General, USMS Director Stacia A. Hylton appointed U.S. Marshal James A. Thompson (D. Utah) to lead an investigation into the allegations made by Chief Inspector Ergas. U.S. Marshal Thompson's investigative report dated July 30, 2014 (summarized below) is attached. It should be noted that the Attorney General has delegated to me authority to review and sign the report, in accordance with 5 U.S.C. § 1213(d).

Sincerely,

Armando O. Bonilla
Associate Deputy Attorney General

Enclosures

2014 AUG 25 PM 4:33
U.S. OFFICE OF
SPECIAL COUNSEL
WASHINGTON, D.C.

AGENCY REPORT SUMMARY
5 U.S.C. § 1213(c) & (d)

1. Summary of Information with Request to which the Investigation was Initiated

By letter dated April 23, 2014, the Office of Special Counsel notified the Department of Justice (DOJ) of whistleblower disclosure allegation under 5 U.S.C. § 1213(a), evidencing a violation of law, rule, or regulation. The allegations were made by U.S. Marshals Service (USMS) Chief Investigator James Ergas, who consented to the disclosure of his name. Currently employed in the USMS Training Academy in Glynco, Georgia, Ergas previously was assigned to the USMS Investigative Operations Division (IOD) in Arlington, Virginia.

The allegation made by Ergas was that the IOD shared drive on the USMS computer network system included unsecured documents – which contained personally identifiable information (PII) – that were improperly accessible to a large number of USMS operation and administrative staff, including contractors and personnel from other divisions and districts. The maintenance of PII in the shared drive, and access to the PII by these persons, were alleged to be a violation of the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and DOJ policies and procedures.

2. Description of the Conduct of the Investigation

Pursuant to the delegation from the Attorney General, USMS Director Stacia A. Hylton assigned a senior-level, Presidentially-appointed U.S. Marshal to conduct an independent investigation. The investigator, U.S. Marshal for the District of Utah James A. Thompson, was granted full access to the USMS computer network and to all USMS personnel, and had full authority to complete the investigation.

At the outset, Thompson had extensive communications with Ergas by telephone and email to allow Ergas to further explain and amplify his allegations, and forward to Thompson supportive documentation. After examining this information, Thompson conducted a full review within the IOD and the USMS Information Technology Division (ITD). Thompson's Investigative Report dated July 31, 2014, is attached.

3. Summary of All Evidence Obtained during the Investigation

ITD authorizes the creation of a shared drive when requested by a division or district office and provides the necessary network capabilities to operate the shared drive. The USMS has formal policies in place requiring that access to PII be limited “to only those individuals who must have such access,” USMS Policy Directive 12.7, and requiring users to “use personal information only in ways that respect an individual’s privacy,” USMS Policy Directive 12.7.2. However, ITD has not promulgated a specific protocol governing what content may be placed on a shared drive, or specific procedures for securing and limiting access to shared drive files. This was left to each division and district office. Following the retirement of the IOD Administrative Officer in 2013, monitoring of the shared drive apparently lapsed, leading to the lack of access controls over the secure files containing PII. The Acting Assistant Director of IOD, once notified of the problem through the OSC letter, took immediate steps to correct the problem.

4. Listing of Any Violation or Apparent Violation of Law, Rule, or Regulation

Inappropriate maintenance of PII is a violation of the Privacy Act, which limits access to records contained in a system of records (such as PII) to only the agency employees “who have a need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1). To constitute criminal conduct, the Act requires “knowing” violations and “willful” disclosure to another. *Id.* § 552a(i). For civil liability, the Act requires an “intentional or willful” violation and only awards “actual damages.” *Id.* § 552a(g)(4). As detailed in his Investigative Report, Thompson did not find evidence of a knowing, willful, or intentional violation of the Privacy Act; nor did he discover any instances of actual inappropriate access to, or disclosure of, PII from the IOD shared drive. Instead, Thompson found that the readily accessible PII on the IOD shared drive was the result of administrative error and required administrative correction.¹

Thompson also found violations of the following DOJ Orders and USMS Policy Directives: DOJ Order 2640.2F, § 2.10 (“Components shall: Reduce the volume of collected and retained PII to the minimum necessary; and Limit access to only those individuals who must have such access.”); USMS Policy Directive 12.7(I) (“USMS staff shall: Reduce the volume of collected and retained PII to the minimum necessary; and Limit access to only those individuals who must have such access.”); and USMS Policy Directive 12.7.2(C)(8) (“Users of Personal Information: Users must acquire and use personal information only in ways that respect an individual’s privacy. This includes: properly destroying personal information contained in hard copy or soft-copy; ensuring that personal information is accurate, timely, complete, and relevant for the purpose which it is collected, provided, and used.”).

5. Description of Any Action Taken or Planned as a Result of the Investigation

A. Change in Agency Rules, Regulations or Practices

As detailed in the Investigative Report (attached), immediate steps have been taken to correct the problem in IOD by removing PII from the shared drive and limiting access within the division. In addition, ITD will be establishing a written protocol for the shared drives USMS-wide to address the issue nationally.

B. Restoration of an Aggrieved Employee

Not applicable.

C. Disciplinary Action Against Any Agency Employee

Inasmuch as the Investigative Report did not find individual culpability, the matter was not referred for disciplinary procedures. Nonetheless, corrective action in IOD was taken and systemic correction is planned.

D. Referral to the Attorney General of any Evidence of Criminal Violation

As stated, Thompson did not find evidence of intentional or willful criminal violations of the Privacy Act of 1974. Accordingly, no referrals for possible criminal action were made.

¹ While the HIPAA is also cited, the federal government is not a “covered entity” under HIPAA privacy rules. P.L. 104-191, Sec. 264; 45 C.F.R. §160.103.

U.S. Marshals Service Investigative Report:
Office of Special Counsel (OSC) File No. DI-14-1514

BACKGROUND

On June 5th, 2014, I was contacted by the U.S. Marshals Service's (USMS) Headquarters and advised I had been designated by the Office of the Director to conduct an investigation into allegations that had been submitted to the Office of Special Counsel (OSC). The allegations involved the failure of employees at the USMS' Investigative Operations Division (IOD) to follow appropriate procedures for safeguarding and disposing of Personally Identifiable Information (PII) and protected health information, in violation of the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, and DOJ Orders.

According to the OSC letter dated April 23, 2014, sent to the U.S. Attorney General, the complainant had indicated that the USMS' IOD management had failed to follow appropriate procedures to safeguard the PII and medical information of USMS IOD employees, Task Force Officers and contractors, by improperly securing folders and files on the IOD shared drive on the USMS' computer system. According to the letter, the complainant, USMS Chief Inspector (CI) James Ergas (GS-1811-14) informed the OSC that the IOD shared drive included "thousands" of unsecured documents containing PII which were available to a large number of current and former USMS employees, contractors and staff from other USMS district and divisions.

In his Whistleblower Disclosure with the OSC, as documented on his submitted Form OSC-12 (Attachment 1), CI Ergas claimed in Part 2: DETAILS OF YOUR DISCLOSURE, 1., that he had personal knowledge of the events and that other employees had told him about events or records involved. (This document was provided to me by CI Ergas, via email on 6/19/14) In section 5. of Part 2; he checked the boxes for violation of law, rule, or regulation, Gross mismanagement and Substantial and specific danger to public safety as to the type of agency wrongdoing that he was alleging.

Further, CI Ergas provided me an attachment (*Attachment A*) to his OSC-12, Part 2; 6., where he specified all the allegations that he was claiming, including, but may not be limited to:

1. Non-secured access of some of the names of individuals that have filed grievances against the agency (in non-encrypted non-password protected) in a file simply named "Grievances"
2. Non-secured access of names and social security numbers of both current and past operational employees, as well as USMS Task Force Officers (TFO) (state, local and federal)
3. Non-secured access to birth dates and location data for IOD personnel
4. Non-secured access to past and current Government Travel Card numbers.
5. Non-secured access to past and current Government Purchase Card numbers
6. Non-secured access to Medical information for IOD operational personnel injured in the line of duty through access to their filed CA-1 and CA-16 paperwork that includes the following: Name,

DOC (presumed to mean DOB), SSN#, home address, dependent information and report of injury

7. Non-secured access to disciplinary files of some IOD Employees with punishment recommendations
8. Non-secured access to home numbers for some IOD Employees
9. Non-secured Federal Express Account information

In the narrative portion of his *Attachment A*, CI Ergas admitted that he has no way of determining when the information was first posted and how much information could "possibly have been copied by and/or removed by personnel no longer employed or contracted by the USMS." He further stated that he has no way of knowing how to gauge the scope of the "potential loss of information." He also indicated that while "former" employees still had access, he was referring to former employees of IOD, currently still employed by the USMS, not retirees.

He further indicated that he was disclosing this information, at the same time, to the USMS' Office of Inspection via Assistant Director Michael Prout and/or Chief Stan Griscavage (USMS' Office of Inspection/ Internal Affairs) stating that he has the utmost confidence in both of them. However, he stated that he felt it necessary to disclose the same information to OSC because he believed it "would be possible that senior USMS Investigative Operations Division leadership would attempt to marginalize the problem" as he believed they had done with other reportable information that CI Ergas has "attempted to bring forward through (his) normal chain of command."

Additionally, in his response to Part 2: 6., he also indicated that he intends to submit an OSC-11 (COMPLAINT OF POSSIBLE PROHIBITED PERSONNEL PRACTICE OR OTHER PROHIBITED ACTIVITY form) in "conjunction with this disclosure on matters involving the same USMS Division."

THE INVESTIGATIVE PROCESS AND CONTACT WITH COMPLAINANT

To gain access to the IOD shared drive to see what types of PII data were accessible, the undersigned first requested access to the shared drive from the Deputy Director of the U.S. Marshals Service, David Harlow (Attachment 2).

Since CI Ergas consented to the release of his name in his communication with OSC, I then contacted him and set up a series of interviews. Telephonic interviews were conducted with CI Ergas on June 12th, June 19th and July 7th, and July 23, 2014. CI Ergas, having recently lateralled from his former position in IOD, phoned in from the USMS's Training Academy in Glynco, GA. Between interviews, there were a series of intermittent emails that had follow-up questions from the previous interview session. In response to one of my questions, trying to get clarification of the unsecured documents to which CI Ergas was referring in the OSC process, CI Ergas mailed me a thumb drive. According to CI Ergas, the contents of the thumb drive were copied from the IOD shared drive while he was still as an IOD employee (prior to his recent lateral his current position). CI Ergas stated that while he still had access

to the IOD shared drive, he had initially accidentally discovered the vulnerable PII information. CI Ergas also sent me a copy of his previously submitted Whistleblower Disclosure form (OSC-12).

The thumb drive contained one large file, entitled *Admin*. The *Admin* file contained 72 folders and 204 documents/spreadsheets. Each of the 72 folders contained sub-folders that contained anywhere from only 1 document to 218 documents/spreadsheets, depending on the folder's topic and dating back as far as 2002. From the data on the thumb drive, it appears that the date that the *Admin* file was copied by CI Ergas was 08/12/13. The dates of the documents within the folders and sub-folders had a variety of dates listed under the column marked "Date Modified", indicating the date that they were either placed in the folder/sub-folder in its original, un-modified condition, or the date when it was saved in its modified/updated version. To discern between the two, one would have to go into the "Properties" of the document to see if there was a difference in the "Created" date and the "Modified" date for each document/spreadsheet. I reviewed the folders, sub-folders, documents and spreadsheets that were contained on the thumb drive to see if I could locate and verify each of the claims made by CI Ergas in his disclosure to the OSC.

Simultaneously, once I had been given access to the IOD shared drive by the ITD, I began to review the files and documents that were contained on the IOD shared drive to compare current IOD employees', TFOs' and contractors' access to the drive and its contents. I also began looking at the files to evaluate the vulnerability of the PII contained on those documents and to see if there was a difference in their availability between the date that CI Ergas copied the documents (08/12/13) and how they are currently posted.

Additionally, on 7/9/14, I contacted the Acting Chief of the USMS' Internal Affairs (IA), Tonia Cline, to have her check IA's records to see if Internal Affairs had investigated, not only any IOD employees, but *any* USMS employees for misuse of PII data that was obtained off any USMS documents. She found no such records, indicating that no one had been reported as having misused any PII data within the USMS.

Once I received the thumb drive sent by CI Ergas, containing the many folders, sub-folders, documents and spreadsheets, all under the large file entitled, *Admin*, I was able to review the content of the files. It quickly became evident that the file that I had been given by CI Ergas did indeed contain numerous documents that contained different combinations of PII data (ie., some had name and DOB; some had name and SSN; or some had name and phone number).

The table shown below is representative, but by no means all inclusive, of the types of files found, the volume of PII data contained within those files, and the combination of the PII data found within these files. All nine of CI Ergas' claims of non-secured data and PII information that he listed in his *Attachment 'A'* on his submitted OSC-12 were found on the thumb drive that he provided to this investigator.

CI Ergas' Admin File→sub-folder→document	PII Data Found
Admin→Telephones + Directory→Office Directory	1 piece of PII data found containing the home address and phone # of an employee who worked out of her home. (There was no indication on the document that this was not an office address, like all the other addresses on this spreadsheet. This was only discovered because I personally know this individual and am aware of her home address.)
Admin→Awards→Performance Appraisals Certification Form	Approx. 400 employees' Annual Performance Rating, w/ their SSNs. Dated 7/26/12
Admin→Awards→2011-12 QSI's	16 employees' names w/ SSNs on spreadsheet (ss) showing the recipients of the limited QSIs
Admin→Awards→Cash Awards	150 names w/ SSNs and \$ amount of awards
Admin→Awards→Time Off Awards	150 names w/ SSNs and # of Time Off hours
Admin→Awards→2008 Performance Award Spread Sheet	80 names w/ SSNs, and \$ amount of cash awards
Admin→Awards→Cash Awards	154 names w/ SSNs and \$ amount of cash awards
Admin→Awards→T.O. Awards	174 names w/SSNs and # of hours of Time Off
Admin→Awards→2011 Perf. Awards IOD	171 names w/ SSN and \$ amount of cash award 172 names w/ SSNs and # of Time Off hours 8 names w/ SSN and showing who got the QSIs
Admin→Awards→2013 Directors Award_GLRFTF	12 names w/ SSNs
Admin→Awards→2013 Dir. Awards.CARTF	2 names w/ SSNs
Admin→Awards→2013 Dir. Award Operation Serge	19 names w/ SSNs
Admin-->Awards-->Dir Award nomination TOG	100 names w/ SSNs
Admin-->Awards-->Appraisals.2006	200 names w/ SSNs
Admin-->Awards-->Award Masterlist	266 names w/ SSNs from 2008 Contained numerous USM-Form 200s required for Time Off Awards
Admin-->Awards-->2011 Performance Awards	161 names w/ SSN and \$ amounts of cash awards
Admin-->Awards--> (employee name)	Numerous examples of this type of file from 204 thru 2013
Admin-->Awards-->Evals-Outstanding 2004-2005	28 names w/ SSNs
Admin-->Awards-->FY 2009 Appraisal Rating List For Awards	300 names w/SSNs and individual performance ratings
Admin-->Badges +Credentials-->IOD 2013 TFO-USM294-Badge Credential Verification	All TFOs assigned to IOD w/badge numbers, approx. 450 employees
Admin-->Badges +Credentials-->IOD 2013 USM294-Badge Credential Verification	All IOD employees w/ badge numbers, approx. 400 names
Admin-->Body Armor-->1811 + Location + SSN	190 IOD employees w/ SSNs (2007)
Admin-->Body Armor-->ISD	190 IOD employees w/ SSNs (2007)

Admin&Clearances&usm561-...	3 individual forms, w/ names, SSN and TS clearance level requested—The top of the form states PRIVACY ACT PROTECTED INFORMATION
Admin-->Credit Cards-->Calling Card Service Transition	96 phone card #s w/names (2010)
Admin-->Credit Cards-->Mex Liaison and Canadian Liaison	26 phone card #s w/ names (2010)
Admin-->Credit Cards-->Credit Card Info.August 2008	174 names w/purchase credit card acct. #s w/ exp. Dates, the last four of their SSNs, and their single/monthly purchase limits
Admin-->Credit Cards-->Credit Card Info December 2008	1 name w/ purchase credit card acct. # w/ exp. Dates, the last four of their SSN, and their single/monthly purchase limit
Admin-->Credit Cards-->IOD Card Holder Listing July 2009	313 TFO and Hqtrs employees w/ cc #s, and mailing addresses for the statements
Admin-->Credit Cards-->IOD Purchase Card list 16 digit 8-1-13	194 purchase card #s, w/ exp. Date and mailing addresses, w/ names
Admin-->Credit Cards--> Purchase Card no comments	174 purchase card #s w/ names, and single/monthly purchase limits
Admin-->Credit Cards-->TFO_travel cards2	Approx. 500 names, travel card #s, SSNs, duty stations (7/30/13)
Admin&Credit Cards->TFO_Travel Cards	Approx. 300 TFO names, cc#s, SSNs and duty stations
Admin&Credit Cards->&Travel Cards Jan 2010	Approx. 70 TOG employee names, w/ travel card #s
Admin->Discipline Files->(name)5-Day Decision 2009	Discipline proposal letter for Senior Insp. (name) listing the penalty and providing details of the offense, case #, but no PII other than name and duty location
Admin->Discipline Files->(name)Decision 2008	Decision Letter for DUSM (name) for a 2-day suspension, provides details of the offense, and the dates that the suspension will take effect. No PII other than Name, title and duty location.
Admin->Discipline Files->Discipline-(name)-Proposed 2-day Suspension	Discipline proposal letter for CI (name) listing the proposed penalty and providing details of the offense, case #, but no PII other than name and division (IOD)
Admin->Duty Roster->Duty Roster06	14 IOD employees' names, office, cell and home phone #s,
Admin->Evaluations->2005PerfAwdNoRat4SUMMARY	50 employee names, w/SSNs, and \$ amount of awards
Admin->Evaluations->2006-2007 Employee Performance Ratings	180 names w/ SSNs and performance rating
Admin->Evaluations->2011-2012 Performance Appraisals	365 IOD employees w/ names, SSNs and perf. Rating
Admin->Evaluations->Appraisal06	218 IOD employees w/ names and SSNs
Admin->Evaluations->Appraisal 2006	215 names w/ SSNs and ratings

Admin→Evaluations→FY 2010 Performance Awards	125 names w/ SSNs, \$ amount of their awards and their performance rating
Admin→Grievances→Chron File- (name)	A chronological account of actions taken surrounding the merit promotion of administrative employee (name)
Admin→Grievances→Chron File- for (name) on (name)	A chronological account of actions taken surrounding the merit promotion of several operational employees, showing names and rankings for different job announcements, and selectees
Admin→Letters→Iraq-CA-1-e-letterhead-letter	Letter written to OWCP regarding an injury sustained by an IOD employee including the employee's name and details of his injury while in Iraq
Admin→Letters→(name)DC Tax Letter (2)	Letter to the TFO, Office of Tax Revenue, D.C., showing employee's name, last four of her SSN, and her home address, including Apt #
Admin→Letters→(name)DC Tax Letter	Same info as above, just a duplicate letter
Admin→Letters→MEMO-interoffice-backgrounds	Security clearance waiver request, with SOIB employee's name, SSN and DOB
Admin→Letters→TS-level request from other agency	Security clearance request letter from another agency, showing the individual's title, name and SSN
Admin→Medical→(name)m1	Shows USM Employee medical Programs notice of Medical Status form w/ employee name and SSN, showing that he is Medically Cleared to perform full range of duties
Admin→Medical→(name)1	Shows USM Employee medical Programs notice of Medical Status form w/ employee name and SSN, showing that he is NOT Medically Cleared to perform full range of duties until he provides additional medical information/documentation
Admin→Medical→(name)1	Shows USM Employee medical Programs notice of Medical Status form w/ employee name and SSN, showing that he is Medically Cleared to perform full range of duties
Admin→OWCP→(name) ECOMP CA1-ECN	E-comp form showing employee's name, home address, DOB, home phone #, nature of injury, and indicates that he has a spouse and children under 18 years
Admin→OWCP→(name) ECOMP CA2-ECN	E-comp form showing employee's name, home address, DOB, home phone #, nature of injury, and indicates that he has a spouse and children under 18 years
Admin→OWCP→(name) ECOMP CA2-ECN *Approximately 20 similar files*	<i>Same type of information as shown in 2 previous files</i>

Admin→Personnel→Clearances	Approx 80 names, w/ security levels, SSNs and duty locations
Admin→Personnel→Clearances-TOG	80 TOG employee names, security levels, SSNs and whether they are an employee or contractor
Admin→Personnel→ClearanceTS SCI(name)	TS-SCI level clearance request, w/ employee name, SSN, and duty assignment
Admin→Personnel→ClearanceTS SCI(name) *numerous similar type letters *	TS-SCI level clearance request, w/ employee name, SSN, and duty assignment
Admin→IOD-Federal Express Accounts	18 FedEx acct. #s, by IOD regional TF office location and the AO of that location

Since I did not know the original source of these IOD-copied files, I had to examine the current IOD shared drive files. I was able to locate a sub-folder entitled *Admin* on the IOD shared drive that appeared to be the source of CI Ergas' files on the thumb drive. After several hours, comparing the files on CI Ergas' thumb drive and the current IOD shared drive, I found the following:

CI Ergas' originally submitted thumb drive with the folder entitled, *Admin*, had 276 folders, documents and spreadsheets. Each of those folders also had hundreds of sub-folders, documents and spreadsheets. By comparison, the current IOD shared drive folder entitled *Admin*, only had 258 folders, documents, and spreadsheets. When I examined the IOD shared drive more closely, I noticed that the more egregious folders and documents containing PII data that were found on CI Ergas' thumb drive (i.e., Allocations, Awards, Badges and Credentials, Body Armor, Certs and USM-577, Clearances, Discipline Files, Evaluations, Grievances, etc.) had been moved into a more secure, protected folder, thus securing the PII content. As my investigation progressed during subsequent days, I found that more and more folders and files had been secured, and that numerous older documents that were no longer needed, had been removed.

I then coordinated my efforts and investigation through a combination of interviews (telephonic and in-person) and e-mail communication with the following personnel from the USMS' Information Technology Division (ITD):

- Shannon Brown, former Assistant Director of ITD
- Tammy Diehl, Chief of Security of the ITD
- Roland Perez-Systems Administrator, ITD

Likewise, numerous interviews, phone conversations and emails between the IOD staff members, senior managers and me were necessary to learn the evolution of IOD's shared drive from its genesis to its current condition. In order to accomplish this aspect of the investigation, I consulted with the following IOD personnel:

- William Snelson-(former) Assistant Director of IOD (Currently the Associate Director of Operations)
- Angel Gonzalez, Acting Assistant Director of IOD
- Denise Levenberry, Administrative Officer, IOD

Joann Lardy, Chief of Policy and Programs, IOD
Jan Conway, Executive Project Manager, IOD

It was learned that as soon as the existence of the unsecured PII data was brought to the attention of IOD management, through the initial notification by the USMS' Office of Internal Affairs of the OSC letter, they recognized the significance of the problem and initiated immediate action. IOD management directed their staff to immediately review of all the folders and documents on the IOD shared drive. They were instructed to eliminate old records that no longer needed to be maintained, to archive those that did need to be maintained, and to secure folders on the shared drive in order to ensure that PII data could not be misused by individuals who should not have access to that data. IOD personnel coordinated their efforts with ITD to evaluate the breadth of the problem and to learn the proper ways to secure the data.

Acting Assistant Director (AAD) Gonzalez' research indicated that his division (IOD) has a 99.9% completion rate for this year's compliance with the USMS' CSAT training requirement. This number indicated that he has only 4 individuals out of a total 410 IOD employees who have not completed the training and his staff is in the process of identifying those individuals to determine whether or not they are still within the IOD or have transferred to a district office.

CREATION OF AND ACCESS TO A USMS SHARED DRIVE

In the most simplistic terms, in order to create a USMS shared drive, a Division or district manager must send a request to the Information Technology Division (ITD) requesting that a new shared drive be set up on the server. The request would require the use of a USM-169, a User Authorization Request form, specifying the name of the shared drive, and a list of folders that need to be on that drive. Each folder should be set up with access "rights or permissions", depending on the employees' needs to access that particular folder. Those parameters enable the Division to control which employees can access each particular folder and restrict those who do not need access.

For example, assume the managers of the *NW Investigators Unit* want to create a new shared drive that could be accessed by all 30 employees assigned to that unit, including the 3 managers. Also assume they want to call the 5 folders on that shared drive, *Current Cases, Closed Cases, Management, Contacts, and Finance*, but they want to restrict the access to two of those folders (*Management and Finance*) to only those personnel who need to access those folders. For the *Management* folder, only the managers (Tom, Mary and Pete) need access. For the *Finance* folder, only the finance officer (Jesse), plus the 3 managers, will need access. All 30 employees will need access to the remaining three folders (*Current Cases, Closed Cases and Contacts*).

In this example, once ITD received the proper request forms, signed by the Division manager, ITD personnel would set up the shared drive similar to the following:

NW Investigators Unit shared drive

Management folder-(can only be accessed by Tom, Mary and Pete)

Finance folder- (can only be accessed by Jesse, plus Tom, Mary and Pete)

Current Cases folder-(can be accessed by all 30 employees, including Jesse, Tom, Mary and Pete)

Closed Cases folder-(can be accessed by all 30 employees, including Jesse, Tom, Mary and Pete)

Contacts folder-(can be accessed by all 30 employees, including Jesse, Tom, Mary and Pete)

Once the shared drive and folders are set up properly, then the authorized users could add documents to the appropriate folders. Those individual documents can also be password protected if the creator of that document does not want others to have access to it. The end result would be that even if you have access to a particular folder, there may still be some documents within that folder to which some users still could not access or could read-only and not modify.

Once this new shared drive was set up properly and in this manner, if one of the investigators, other than the managers (Tom, Mary or Pete) tried to access the *Management* folder, he would get an error message, saying that he was not authorized access to that folder. Likewise, if one of the employees other than Jesse, Tom, Mary or Pete, tried to access the *Finance* folder, he would receive the same error message.

As employees come and go, through promotions, retirements, transfers or even if their job requirements changed, the permissions to those folders would have to be constantly managed to ensure the integrity of the system. Management of those changes requires the vigilance of at least two entities—the IOD management representative and an ITD staff member that is needed to add/remove one's access. Additionally, over time, more folders could be added to the originally built shared drive, but those, too, would have to be set up with the proper permissions, as were the first five folders. Either of these functions would require that an authorized individual contact ITD each time that there was a need to modify access to those folders. The proper way to modify access to the folders or the shared drive is by the submission of a User Access Request (USM-169). The UAR would provide a record of the modification as required by DOJ(Order 2640.2F, 2.,c.,(1)) and USMS (Policy 17.2, 2. H.(2)) policies.

HOW DID THE IOD SHARED DRIVE GET TO THE POINT THAT THE FOLDERS CONTAINING PII DATA WERE IN UNSECURED FOLDERS?

The IOD personnel that were interviewed (listed above) would normally be the key personnel to answer that question. However, none of the IOD personnel listed above were employed in their current capacity at the time that the original IOD shared drive was created. None of the interviewees could even provide the name of any current IOD employee that would still be available to explain how the original IOD shared drive was created. Nor were any of the interviewees able to explain why so many

documents were available to such a wide array of IOD personnel. Although each interviewee understood that folders and files could be secured, they were unfamiliar with the technical process of doing so. Each of the interviewees had been recently made aware of the vulnerability of these records through senior IOD managers and they were all very concerned about the problem. They recognized the significance of the problem and recognized the availability of the PII data as a violation of USMS policy, largely due to their annual requirement of reading, reviewing and acknowledging the USMS' Rules of Behavior (USMS Policy 12.7.2) and DOJ's Computer Security Awareness Training (CSAT)(USMS Policy 12.7.1 M.1.a.)

Several IOD interviewees suggested that when the former Administrative Officer (AO) Deb Miller retired over a year ago, some of the permissions to the folders may have been changed so that her previously secured folder contents could be retrieved in her absence. (Ms. Miller had a reputation, according to her co-workers, of running a tight ship and would have known not to post unsecured PII data where others could have had access). Within the USMS, the AO is the person frequently tasked with many of the Human Resources type of activities and that would handle documents including the tracking of awards, contact numbers, CA-1 forms, credit card information, etc. Many of the more egregious documents found by CI Ergas were these types of documents. (See Chart above).

Retired AO Deb Miller was contacted and she indicated as follows. She stated that as the AO, she had several folders on the IOD shared drive to which access was restricted to her and a small number of her staff members with a need to access certain documents that contained PII. She indicated that restricted access was in place as far as she could tell at the time of her retirement. After the recent issue raised about the shared drive was explained to her, Deb Miller shared her recollection of a similar time in the 2011-2012 timeframe during an ITD upgrade of the USMS network when the restricted folders had inexplicably become unrestricted similar to the recent discovery. She became aware of the situation and promptly coordinated with ITD and had the restrictions and password protections re-established. If that had reoccurred and not been corrected, PII may have remained unrestricted.

Even CI Ergas, the complainant, admitted that in years past, while he was still assigned to the IOD, he had not seen the volume of unsecured data that he saw when he captured the *Admin* folder lending credibility to the possibility that the folder "permissions" may have changed at the time of the departure of the former AO.

Additionally, it was learned that it is very labor intensive to maintain the access of current employees as they come into and exit the IOD. IOD is one of the largest divisions within the USMS with over 400 personnel, including government employees, Task Force Officers (TFOs), contractors and interns. Their individual lengths of service within IOD before they are transferred, promoted or retired, varies significantly, requiring constant monitoring of computer access and the filing of UARs. This applies not only at the headquarters offices within the IOD, but also in their many field offices, foreign and domestic. The UARs are frequently completed by personnel that were not assigned to IOD at the beginning of the employees' start within IOD, so they would be unaware of what previously issued access the individual employees may have had.

Combine that system flaw with the fact that, over a period of time, according to ITD personnel, it would be quite possible for an individual employee to have un-cancelled access from his/her previous position, simply by the authorized signer cancelling one's *current* access, not being familiar with that same employee's *previous* access. The records that were found in the *Admin* folder went back to at least 2002. During the time period between 2002 and the time that the *Admin* folder was copied, numerous personnel had come and gone, as had the IOD managers, both at headquarters and in the field offices, who would have been the authorized signers of the UARs as had the ITD personnel who would have facilitated the access initiation/cancellations.

Interviews with ITD security staff revealed similar activities within ITD to review current procedures and to seek solutions to their inefficient and flawed methods of monitoring changes in personnel. Even with the current system of requiring a UAR form for each modification to access or permissions, frequently previous permissions were not cancelled. The end result would be that personnel whose position requirements changed, may still have access to folders and documents that they no longer require. In looking within their own ranks, ITD security personnel found that in some cases, some of their own personnel still had access to folders to which they no longer managed. Fortunately, USMS and DOJ policies require ITD personnel to annually read and acknowledge receipt of the enhanced Rules of Behavior for "privileged" employees. Additionally, when IOD asked ITD to give them an accurate list of the current access of each of the IOD personnel, ITD realized that the task would require a manual search of all previously issued UARs, by name. They would then have to compare it to a list of current IOD employees, followed by a search of permissions assigned to each shared drive and individual folders. This process would be very labor intensive, time consuming and subject to oversight errors, due to the sheer volume of documentation and employees assigned to the IOD.

CURRENT AND PLANNED CORRECTIVE ACTION

IOD took immediate action to research the problem by reviewing their shared drive and the folders and files contained within. They quickly reached out to ITD for assistance to help them determine how they needed to proceed to correct the exposed folders. According to the Memorandum from AAD Gonzalez, dated July 25, 2014, "there has been an ongoing effort since June 2014 to identify and restrict access to old information containing PII as well as current information containing PII (Attachment 3, Section 8.)." IOD personnel began to transfer files from unsecured folders into "protected" folders and "locked down" other folders that were unsecured. They identified documents that were no longer needed and began to archive those that needed to be saved. Some folders containing administrative documents have now been grouped together in restricted folders. Ten older folders, containing old data that did not need to be archived, have been eliminated altogether. According to AAD Gonzalez, IOD personnel quickly identified three folders that contained unsecured PII data including SSNs and corresponding passport numbers. Those folders are now restricted.

IOD even went so far as to also identify a folder used by the International Investigations Branch that contained investigative PII data for *criminal subjects*, as opposed to PII data of USMS personnel, and

restricted access to this type of file, too, even though that was not as critical. (This type of folder would typically be shared by investigators working on the same case.)

The Executive Support Staff reviewed unrestricted folders on the shared drive in an effort to identify additional unsecured PII data. They found award nomination forms, whose outdated business practice included the requirement of listing the full SSN of the recipients, and modified those forms to eliminate the PII data contained within. Other folders, belonging to two Senior Inspectors were identified, and have been moved to their individual, personal H drive, or locked down.

Additionally, for the past several years, the Executive Support Staff has worked with all IOD branches to create team collaboration sites on SharePoint and has encouraged users to place documents in SharePoint rather than on the shared IOD drive. According to AAD Gonzalez, permissions are easier to control on the SharePoint platform.

AAD Gonzalez plans to broaden IOD's efforts by having each Branch Chief oversee a cleanup of old information that can be archived or deleted entirely from their shared drive folders beginning in August of 2014 (some of the Regional Task Force offices have their own shared drive, in addition to the IOD headquarters shared drive.) (Attachment 4) IOD intends to generate new guidelines for all IOD management and staff, enlisting the services of the Records Management Specialist to ensure that records are not improperly deleted that should, instead, be saved for archival purposes. Additionally, the new guidelines will provide specific instructions for IOD personnel for future posting of folders or files on the shared drive.

ITD is currently working with IOD management and staff to eliminate the unsecured and readily accessible PII data that was discovered. ITD's assistance is needed to prevent the accidental loss of important data and to ensure that those who need access to certain files, don't lose their appropriate level of access. At the same time, ITD security personnel are reevaluating their internal procedure to ensure compliance with DOJ and USMS information technology Orders and Policies. They are working towards a USMS wide protocol for USMS shared drives that will govern the content of data placed in USMS shared drives, limitations on PII, and access limits to secure files.

Additionally, it was learned that ITD was already working toward obtaining an access program that is Windows based that will be able to terminate all access for an individual when the employee moves, retires, or whose access needs change. The program will significantly improve the management of USMS systems access by providing a system that will reduce the current labor intensive processes. ITD also recognizes that the personnel changes over time, including ITS management positions, have made it difficult to keep up with coordination efforts from each of the headquarters components and the districts field offices.

ADDITIONAL OBSERVATIONS:

As a senior investigator for the USMS, a senior manager for the USMS and a daily user of the IT systems, it is the opinion of this investigator that a major contributing factor in this case of accessible PII data is the lack of a strong and recurring educational IT training program, other than the current annual DOJ CSAT and USMS Rules of Behavior review. While both of these training tools address the need and requirement to protect PII data within the curriculum, neither goes far enough to address *how* individuals and managers need to initially set up shared drives and folders in a secure manner, nor does it sufficiently address *how* managers are to manage the shared drives once they have been created. Although each of the following policies specifically address either the protection of PII data or access control, most employees overlook the specific references as the policies are quite complex:

DOJ Order 2640 2F-Information Technology Security, Section 5.b., Access Control, and Chapter 2. 10., Sensitive and Personally Identifiable Information

DOJ 2880.1C, Information Resources Management Program, Section 10. IT Security Management, a., b. and c., and Section 13. a. Protection of Privacy and personally Identifiable Information (PII)

USMS Policy 12.7, IT Security, 9. Technical Security Policy, a. Access Control, h., Personnel Security, and I., Sensitive and Personally Identifiable Information (PII)

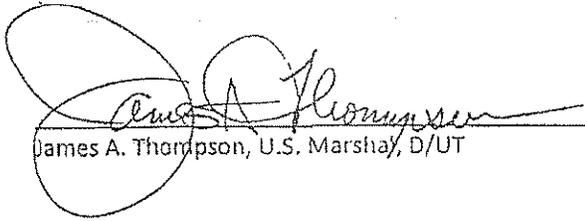
USMS Policy 12.7.1, USMS IT Security Procedures, F. Personnel Security; and M. Security Awareness, Training, and Education, 1. Employee Awareness, and 2., IT professional Training

USMS Policy 12.7.2 Rules of Behavior, C. 8., Users of Personal Information and D., System Access and Use.

Since it is the DOJ and USMS requirement that every IT user abide by the policies listed above, every employee needs to know how to accomplish this task so that all future data will be properly secured. This would also be helpful as the employees are promoted up into management positions to help insure the integrity of the systems.

An enhanced training program was recommended as part of the solution to the ITD Security Chief, who confirmed that she plans to initiate such a program within her assigned division and for the benefit of the entire USMS. Although *no cases* involving the misuse of PII data have ever occurred within the USMS to date, the enhanced training program will help to ensure that there are no future opportunities for such an offense.

And finally, I found no intent by anyone to misuse the unsecured PII data. Nor did I find any victims of identity theft that resulted from the temporarily exposed PII data that was available on the IOD shared drive. I found no evidence that PII had actually been accessed and disclosed improperly by anyone. However, the evidence is clear that PII was accessible in an improper fashion.


James A. Thompson, U.S. Marshal, D/UT

7/30/14
Date

U.S. OFFICE OF SPECIAL COUNSEL
Form OSC-12

(202) 254-3640 / (800) 672-2249
OMB Control No. 3255-0002
Exp. Date: 2/28/14

INFORMATION ABOUT FILING A WHISTLEBLOWER DISCLOSURE
WITH THE
OFFICE OF SPECIAL COUNSEL

IMPORTANT

Before filling out this Office of Special Counsel (OSC) Disclosure of Information form, please read the following sections about limitations on OSC's jurisdiction over whistleblower disclosures. Only the most frequently occurring impediments to OSC jurisdiction are described. OSC may not have jurisdiction over you or your disclosure for other reasons not discussed below.

COMPLETED DISCLOSURE FORMS CAN BE SENT TO OSC BY MAIL, AT: DISCLOSURE UNIT, OFFICE OF SPECIAL COUNSEL, 1730 M STREET, N.W. (SUITE 218), WASHINGTON, DC 20036-4505. OR BY FAX: 202-254-3711

PLEASE KEEP A COPY OF DISCLOSURE MATERIALS PROVIDED TO OSC. REPRODUCTION CHARGES UNDER THE FREEDOM OF INFORMATION ACT MAY APPLY TO REQUESTS PROCESSED BY OSC FOR COPYING OF COPIES OF MATERIALS IN OSC FILES.

OSC WHISTLEBLOWER DISCLOSURE CHANNEL

The OSC Disclosure Unit serves as a secure channel that can be used to disclose -

- a violation of law, rule or regulation;
- gross mismanagement;
- gross waste of funds;
- abuse of authority, or
- substantial and specific danger to public health or safety.

OSC does not have authority to investigate the disclosures that it receives. The law provides that OSC will (a) refer protected disclosures that establish a substantial likelihood of wrongdoing to the appropriate agency head, and (b) require the agency head to conduct an investigation, and submit a written report on the findings of the investigation to the Special Counsel.

If OSC finds no substantial likelihood that the information discloses one or more of the categories of wrongdoing, the Special Counsel must: (a) inform the whistleblower of the reasons why the disclosure may not be acted on further; and (b) direct the whistleblower to other offices available for receiving disclosures.

OSC JURISDICTION

The Disclosure Unit has jurisdiction over federal employees, former federal employees, and applicants for federal employment. It is important to note that a disclosure must be related to an event that occurred in connection with the performance of an employee's duties and responsibilities. The Disclosure Unit has no jurisdiction over disclosures filed by:

VISIT [HTTP://WWW.OSC.GOV](http://www.osc.gov) FOR MORE INFORMATION ABOUT
OSC JURISDICTION AND DISCLOSURE PROCEDURES

**INFORMATION ABOUT FILING A WHISTLEBLOWER DISCLOSURE
WITH THE OSC (cont'd)**

- employees of the U.S. Postal Service and the Postal Rate Commission;
- members of the armed forces of the United States (i.e., non-civilian military employees);
- state employees operating under federal grants; and
- employees of federal contractors.

FIRST-HAND INFORMATION REQUIRED

In order to make a "substantial likelihood" finding (*see previous page*), OSC must be in possession of reliable, first-hand information. OSC cannot request an agency head to conduct an investigation based on an employee's (or applicant's) second-hand knowledge of agency wrongdoing. This includes information received from another person, such as when a fellow employee informs you that he/she witnessed some type of wrongdoing. (Anyone with first-hand knowledge of the allegations you want to report may file a disclosure in writing directly with OSC.) Similarly, speculation about the existence of misconduct does not provide OSC with a sufficient legal basis upon which to send a matter to the head of an agency. If you think that wrongdoing took place, but can provide nothing more than unsubstantiated assertions, OSC will not be able to go forward with the matter.

DE MINIMIS ALLEGATIONS

While an allegation might technically constitute a disclosure, OSC will not review or refer *de minimis* or trivial matters.

ANONYMOUS SOURCES

While OSC will protect the identity of persons who make disclosures, it will not consider anonymous disclosures. If a disclosure is filed by an anonymous source, the disclosure will be referred to the Office of Inspector General in the appropriate agency. OSC will take no further action.

MATTERS INVESTIGATED BY AN OFFICE OF INSPECTOR GENERAL

It is the general policy of OSC not to transmit allegations of wrongdoing to the head of the agency involved if the agency's Office of Inspector General has fully investigated, or is currently investigating, the same allegations.

DISCLOSURE OF INFORMATION

(Please print legibly or type and complete all pertinent items. Enter "N/A" (Not Applicable) or
"Unknown" where appropriate.)

PART 1: BACKGROUND INFORMATION

1. Name of person seeking OSC action ("Complainant"): Mr. Ms. Mrs. Miss
 James Ergas

2. Status:
 Current Federal employee Applicant for Federal employment
 Former Federal employee Other (please specify):

3. Contact Information:
 Home or mailing address:

 Telephone number(s): () () (Home)
 () () (Office) Ext.
 (Cell)
 Fax number: ()
 E-mail address:

4. Current position, title, series, and grade:
 Chief Inspector, GS-1811-14

5. Agency Name: United States Marshals Service

6. Agency Address:
 Crystal Square
 Arlington, VA 22215

7. How did you first become aware that you could file a disclosure with OSC?
 OSC brochure OSC poster OSC speaker OSC web site
 Agency personnel office Union Co-worker News story
 Other (please describe):
 Date (approximate): Not sure

DISCLOSURE OF INFORMATION
 Page 2

8. If you are filing this complaint as a legal or other representative of the person making a disclosure, please supply the following information:
 Name / title of filer: Mr. Ms. Mrs. Miss

9. Contact Information:
 Home or mailing address:

 Telephone number(s): () () (Home)
 () () (Office) Ext.

Handwritten text, possibly a signature or name, located in the center of the page. The text is faint and difficult to read.

Fax number: ()
E-mail address:

PART 2: DETAILS OF YOUR DISCLOSURE

- 1. I know about the information I am disclosing here based on *(check all that apply)*:
 I have personal and/or direct knowledge of events or records involved ()
 Other employees have told me about events or records involved ()
 Other source(s) ()
(please explain):

2. Please identify the U.S. government department or agency involved in your disclosure:
United States Marshals Service

3. Please identify the organizational unit of the department or agency involved:
Investigative Operations Division

4. Address of the organizational unit:
Crystal Sq, Arlington, VA 22215

5. Please identify the type of agency wrongdoing that you are alleging *(check all that apply)*. If you check "violation of law, rule, or regulation," please provide, if you can, the particular law, rule or regulation violated (by name, subject, and/or citation).

Violation of law, rule, or regulation () *(please specify):* Personally Identifiable Info.

DOJ Order 2880, IC, DOJ Order 2640.2F, and OMB M-07-16

Gross mismanagement () Gross waste of funds () Abuse of authority ()
Substantial and specific danger to public health ()
Substantial and specific danger to public safety ()

DISCLOSURE OF INFORMATION
Page 3

6. Please describe the agency wrongdoing that you are disclosing, indicating how the agency's actions fit within the type(s) of wrongdoing that you checked in item 5. *(Be as specific as possible about dates, locations and the identities and positions of all persons named. Also, please attach any documents that might support your disclosure. Continue on a separate sheet of paper if you need more space.)*

Please See Attachment 'A'

Additionally, an OSC-11 will also be filed in conjunction with this disclosure on matters involving the same USMS Division.

DISCLOSURE OF INFORMATION
Page 4

PART 3: OTHER ACTIONS YOU ARE TAKING ON YOUR DISCLOSURE

1. I have previously disclosed (or am disclosing) the violations alleged here to (*complete all that apply*):

- Inspector General of department / agency involved Date: / /
- Other office of department / agency involved Date: / /
(*please specify*):

- Department of Justice Date: / /
- Other Executive Branch / department / agency Date: / /
(*please specify*):

- () General Accounting Office (GAO) Date: / /
- () Congress or congressional committee Date: / /
(please specify member or committee):
- () Press / media (newspaper, television, other) Date: / /
(please specify):

2. If you disclosed the information reported here through any other channel described in question 1, above, what is the current status of the matter?

PART 4: CONSENT, CERTIFICATION, AND SIGNATURE

Do you consent to the disclosure of your name to others outside the Office of Special Counsel if it becomes necessary in taking further action on this matter?

I consent to disclosure of my name:

Signature James M Engao Date 16 Dec 2013

I do not consent to disclosure of my name:

Signature _____ Date _____

DISCLOSURE OF INFORMATION
Page 5

I certify that all of the statements made in this complaint (including any continuation pages) are true, complete, and correct to the best of my knowledge and belief. I understand that a false statement or concealment of a material fact is a criminal offense punishable by a fine of up to \$10,000, imprisonment for up to five years, or both. 18 U.S.C. § 1001.

Signature James M Engao Date 16 Dec 2013

PART 5: PRIVACY ACT / PAPERWORK REDUCTION ACT STATEMENTS

Routine Uses. Limited disclosure of information from OSC files is needed to fulfill OSC's investigative, prosecutorial and related responsibilities. OSC has described 18 routine uses for information in its files in the *Federal Register* (F.R.), at 66 F.R. 36611 (July 12, 2001), and 66 F.R. 51095 (October 5, 2001). A copy of the routine uses is available from OSC on request. A summary of the routine uses appears below.

OSC may disclose information from its files in the following circumstances:

- 1. to disclose that an allegation of prohibited personnel practices or other prohibited activity has been filed;

2. to disclose information needed by the Office of Personnel Management (OPM) for inquiries involving civil service laws, rules or regulations, or to obtain an advisory opinion;
3. to disclose information about allegations or complaints of discrimination to entities concerned with enforcement of anti-discrimination laws;
4. to the MSPB or the President, when seeking disciplinary action;
5. to the involved agency, MSPB, OPM, or the President when OSC has reason to believe that a prohibited personnel practice has occurred, exists or is to be taken;
6. to disclose information to Congress in OSC's annual report;
7. to disclose information to third parties (without identifying the complainant unless OSC has the complainant's consent) as needed to conduct an investigation; obtain an agency investigation and report on information disclosed to the OSC whistleblower disclosure channel; or to give notice of the status or outcome of the investigation;
8. to disclose information as needed to obtain information about hiring or retention of an employee; issuance of a security clearance; conduct of a security or suitability investigation; award of a contract; or issuance of a license, grant, or other benefit;
9. to the Office of Management and Budget (OMB) for certain legislative coordination and clearance purposes;

DISCLOSURE OF INFORMATION
Page 6

10. to provide information from an individual's record to a congressional office acting pursuant to the individual's request;
11. to furnish information to the National Archives and Records Administration for records management purposes;
12. to produce summary statistics and work force or other studies;
13. to provide information needed by the Department of Justice for certain litigation purposes;
14. to provide information needed by courts or adjudicative bodies for certain litigation purposes;
15. to disclose information to the MSPB as needed in special studies authorized by law;
16. for coordination with an agency's Office of Inspector General or comparable entity, to facilitate the coordination and conduct of investigations and review of allegations;
17. to news media or the public in certain circumstances (except when the Special Counsel determines that disclosure in a particular case would be an unwarranted invasion of personal privacy); and
18. to the Department of Labor and others as needed to implement the Uniformed Services Employment and Reemployment Rights Act of 1994, and the Veterans' Employment Opportunities Act of 1998.

Purposes, Burdens, and Other Information. An agency may not conduct or sponsor a collection of information, and persons may not be required to respond to a collection of information, unless it (a) has been approved by OMB, and (b) displays a currently valid OMB control number. The information in this form is collected pursuant to OSC's legal responsibility (at 5 U.S.C. § 1213) to receive disclosures from current or former federal employees, or applicants for

Attachment 'A'

Response to Question 6

The current United States Marshals Service (USMS) Assistant Director for the Investigative Operations Division (IOD) is William Snelson.

There are currently hundreds if not thousands of unsecured pieces of Personally Identifiable Information (PII) within IOD's shared drive. I have no way of knowing how to gauge the scope of the potential loss of information.

This information is currently available to anyone who has or has had access to IOD's shared drive since the information was posted and it appears that the information has been posted at different times by different people.

Access could include an unknown number of past and current USMS Operational Personnel, USMS Administrative Personnel, contract personnel, personnel from other USMS districts and divisions, and may also include access by outside agency personnel. Additionally, since virtually none of the data is either password protected or encrypted it would appear reasonable to believe that numerous ITD employees and ITD contract personnel would be able to access the information through their systems.

The information includes but may not be limited to the following:

1. Non-secured access of some of the names of individuals that have filed grievances against the agency (in a non-encrypted non-password protected) in a file simply named "Grievances"
2. Non-secured access of names and social security numbers of both current and past operational employees, as well as USMS Task Force Officers (TFO) (state, local and federal).
3. Non-secured access to birth dates and location data for IOD personnel (very disconcerting when combined with other easily accessed PII such as employee and TFO ssn#'s).
4. Non-secured access to past and current Government Travel Card numbers.
5. Non-secured access to past and current Government Purchase Card numbers.
6. Non-secured access to Medical information for IOD operational personnel injured in the line of duty through access to their filed CA-1 and CA-16 paperwork that includes the following: Name, DOC, SSN#, home address, dependent information and report of injury.
7. Non-secured access to disciplinary files of some IOD Employees with punishment recommendations.

AME
16 Dec 2013

8. Non-secured access to home numbers for some IOD Employees

9. Non-secured Federal Express Account information

With respect to encryption and password protection of documents there are several that are password protected within the data base so it clearly has the capability.

I have no way of determining when the information was first posted it would be impossible to determine how much of the information could have possibly been copied by and/or removed by personnel no longer employed or contracted by the USMS. I would, also guess that it is possible that even interns may have had access to the information if they are permitted access to IOD's shared drive.

The information is not hidden and is easily accessible by anyone who has access to IOD's shared drive. Additionally, to fully understand the breadth of the breach, IOD had hundreds of employees and hundreds of TFO's stationed around the country. Since the data is not secured anyone at any time with in the division or anyone who has been provided access to IOD's shared drive could have viewed or copied it.

I am disclosing this to you at the same time I am disclosing it to our Office of Inspection via Assistant Director Michael Prout and/or Chief Inspector Stan Griscavage. I have the utmost confidence in both AD Prout and Chief Griscavage. I feel that I must also disclose the information to you as I believe that it is possible that senior USMS Investigative Operations Division leadership would attempt to marginalize the problem and not have it properly investigated as I believe they have done with other reportable information that I have attempted to bring forward through my normal chain of command.

Please review this report alongside the OSC-11 form that I will also be submitting.

POC: James Ergas, Chief Inspector, United States Marshals Service .

AME
16 Dec 2013



ATTACHMENT 2

6/11/14 - SEARCHED +
E-MAIL TO
AD. BROWN.

U.S. Department of Justice
United States Marshals Service
Information Technology Division

Washington, D.C. 20530-1000

MEMORANDUM TO: David Harlow
Deputy Director
United States Marshals Service

FROM: James Thompson 
United States Marshal
District of Utah
United States Marshals Service

VIA: Shannon Brown
Assistant Director for Information Technology,
Chief Information Officer
United States Marshals Service

SUBJECT: USM Thompson, D/UT Request for Employee Email / Internet Usage Log Files and access to the IOD Shared Drive.

USM James A. Thompson of the D/UT is requesting to obtain approval to potentially receive the email and /or Internet usage log files of Chief Inspector James Ergas in support of an inquiry from the U.S. Office of Special Counsel. Additionally, USM Thompson is requesting access to the shared drive of IOD to validate information in the complaint.

The request is to receive email and/or Internet usage log files for an unknown period of time. Specifics will be provided later this week as the needs are determined. This request is to initiate the process of gaining access. Efforts are/will be coordinated through A.D. Brown and her security staff.

USMS Directive 12.2.D.3 authorizes the release of this information in support of allegations of violations of system security with the approval of the Deputy Director or Director of the USMS.

Background:

This investigation was authorized and requested by the Office of the Director/Deputy Director via the USMS' Office of General Counsel in response to an inquiry by the U.S. Office of Special Counsel.

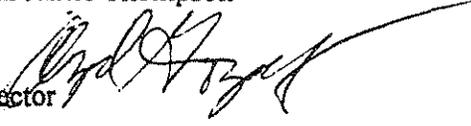
ATTACHMENT 3



U.S. Department of Justice
United States Marshals Service
Investigative Operations Division

Alexandria, Virginia 22301-1025

July 25, 2014

MEMORANDUM TO: United States Marshal James Thompson
FROM: Angel Gonzalez
Acting Assistant Director 
SUBJECT: Investigative Operations Division Review of Share Drive

The following is in response to your recent inquiry and specific questions regarding the Investigative Operations Division's (IOD) shared drive processes and the accessibility of Personally Identifiable Information (PII) on the shared drive:

1. Within IOD, who is normally given access to the IOD shared drive?

Within IOD there are varied levels of employees who receive access to the IOD Headquarters (HQ) Shared Drive, including FTE positions assigned to an IOD HQ located entity, Contractors who perform jobs that require access to folders maintained on the shared drive, and interns who will perform work that requires access to a folder maintained on the shared drive. Some RFTF employees and contractors also have been granted access to the IOD HQ Shared Drive if their responsibilities are such (i.e. Fleet) that they require access to a folder on that drive. Access to the IOD HQ shared drive by IOD employees located in an off-site field location is minimal, as most Regional Fugitive Task Forces (RFTF) also have a shared drive for their specific RFTF location. Generally, that RFTF access is for senior level supervisory personnel at the RFTF as well as their contractors who perform jobs where information is contained on the IOD Shared Drive. Additionally, all Sex Offender Investigations Branch Regional Field Chiefs have access to the IOD shared drive.

2. Within IOD, is there a minimal security clearance level?

IOD follows USMS policy for clearances and background investigation standards. The Tactical Operations Division (TOD) manages the background check of any employee entering service within IOD and the level of clearance or background performed and granted follows HSPD-12 guidelines. Positions that require an actual clearance do

receive that. Positions that require only a background check and public trust designation receive that. IOD does request that a Top Secret Clearance be granted for any position that requires it but does not request them for every position, i.e., contractors or interns. IOD follows USMS TOD policy and procedure for any position not designated to be in need of a clearance or higher level clearance. No one who has not received his or her authorization to have a JCON account issued is ever allowed access to any USMS or IOD database or drive.

- 3. Within IOD, what levels of security clearances are assigned to personnel that have access to the shared drive? Or does it vary?**

Clearance levels within IOD vary with positions. There is no requirement that a certain level of any clearance be granted prior to access to a shared drive. According to information obtained from the USMS Information Technology Division (ITD), the USMSNet Security directive states that PII is stored on USMS shared drives. ITD also states that there is *no formal written procedure* for how to handle the storage of PII. However, ITD advises that the *known procedure* is to create a folder on the shared drive where the PII information is to be stored and create a USM-169 that locks down that folder to only those who need access. IOD plans to work with our assigned ITD Technical representative to include a written procedure for this process in our Standard Operating Procedure (SOP) for IOD Shared Drive access and use.

- 4. What is the normal procedure to authorize an IOD employee access to the IOD shared drive? (Who authorizes it, who submits the USM-169, who monitors the addition/deletion of the access as employees transfer into IOD and out of IOD through promotions, retirements, etc?)**

Personnel entering IOD receive a packet of information and forms to complete from the Administrative Officer (AO) prior to entry into IOD. This includes the submission of a USM-169 to either create or transfer a JCON account. If a person is to be granted access to a shared drive, the AO may sign this for an FTE. Generally all IOD employees entering the division at a HQ located office (i.e., CS3/CS4/Bell Street) are granted access as all branches maintain folders on the shared drive. It is IOD's practice for the AO to sign all USM-169s for new employees as well as for existing employees who need additional access to accounts, such as JDIS, JSRA, certain Outlook folders, etc. However, some USM-169 forms have been submitted to ITD by Branch Chiefs or field Chiefs or their designee for those positions working within their jurisdiction. This procedure will be clarified in the IOD SOP. Employees who move from the division or who leave the USMS entirely are submitted for transfer or removal of their account through the ITD USM-169 process.

- 5. What is IOD's compliance level with the annually required CSAT/Rules of Behavior training?**

IOD has a 99+% rate of CSAT compliance. Of 410 employees, only four did not complete CSAT training by the required date. ITD provided those names to us. Two employees are on extended administrative leave and have not been in a USMS facility

since prior to the CSAT requirement. One is on maternity leave and will be scheduled to complete the training when she returns. And one is on extended TDY to the Philippines and currently does not have access to USMS systems.

6. Who (by position) would normally place documents/folders onto the shared drive?

All IOD personnel in all positions with access (i.e., FTE, contractor, intern) may place documents into shared drive folders. Interns are usually tasked with jobs like updating and maintaining Memoranda of Understanding or signed Rule of Behavior, etc., and must then update the folder. They also upload documents from districts regarding investigations like 15 Most Wanted cases. These administrative duties have been assigned to interns for some time and require access to the shared drive. Contractors generally interact with the folders that contain their program area, i.e. Fleet.

7. Does IOD have an IT person (SA) specifically assigned to IOD?

There are some Systems Administrators (SA) assigned to RFTF areas due to their geographic location (for example, they cover an RFTF if they also cover that district location) and IOD has an ITD Technical Representative (Todd Gerstner) who serves as the IOD/ITD POC. There is no one overall SA from ITD for the entire division. The following personnel support the RFTFs:

Florida/Caribbean – Dave Young
Great Lakes – Keith Feejoo
Gulf Coast – Rick Bullard
New York/New Jersey – Stan Li

8. Are there some old records containing PII information on the shared drive that can be locked down or eliminated altogether?

There has been an ongoing effort since June 2014 to identify and restrict access to old information containing PII as well as current information containing PII. Some folders have been password protected and some have been placed on restricted access with a USM-169 submission being necessary to gain access to those folders within the shared drive. The AO found several folders containing administrative documents that were all grouped together into one main Admin folder and access to that folder is restricted to three personnel within IOD. The AO also deleted approximately 10 folders containing prior year information that was more than seven years old and unnecessary to maintain.

The Executive Support Staff reviewed unrestricted folders on the shared drive in an effort to identify possible PII. Old Director's Awards nomination forms that contain Social Security Number (SSN) as a business practice were amended so that the nomination form is retained but the SSNs have been deleted. Two Senior Inspectors who had folders on the shared drive that contained PII information were notified and those folders were either deleted, moved to a personal H drive, or locked down.

In July 2014, IOD identified three additional folders that contained potential PII (SSNs and passport numbers) that were then placed into restricted access. IOD also identified a folder used by the International Investigations Branch that did not need to have general access and that was submitted for restricted access with an identified group of users. This folder did not contain personnel PII but did contain investigative data for criminal subjects.

Two folders that should have been maintained on an employee's H drive as opposed to the IOD Shared Drive were located and moved. These folders contained only submitted forms for building access but did include SSNs. Those folders are no longer on the shared drive. IOD has also redacted some documents to remove PII. These documents were all related to Award submissions and ratings. These documents will be moved to the restricted Admin folder now that that rating cycle is complete and no further general access to these documents is necessary.

Future Activity for Controlling the Shared Drive

For several years, the Executive Support Staff has worked with all IOD Branches to create team collaboration sites on SharePoint and has encouraged users to place documents in SharePoint rather than on the shared drive. Permissions are easier to control on the SharePoint platform and do not require the submission of a USM-169.

A new effort that will require each Branch Chief to oversee a clean-up of old information that can be archived or deleted entirely from their Shared Drive folders is scheduled to begin August 01, 2014. Prior to doing this clean-up and archiving of information, folders and/or documents IOD will generate guidelines for the term of time information should be available on the shared drive and how to adequately and correctly determine what should be archived and what can be deleted entirely. The IOD Records Management Specialist will be enlisted in this effort to ensure that IOD does not improperly delete records that must be maintained through an archival process. A memo to the field explaining shared drive processes and the need to restrict information such as PII from being placed into a general access folder will be issued from the AD to all IOD employees in advance of this effort.

The current status of the IOD Shared Drive is:

Total size:	348GB (gigabyte)
Number of folders:	50,689
Number of files:	357,726
Average folder size:	7.02MB (megabyte)
Average file size:	1,019KB (kilobyte)



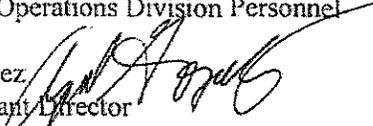
Attachment 4

U.S. Department of Justice
United States Marshals Service

Investigative Operations Division

Alexandria, Virginia 22301-1025

July 30, 2014

MEMORANDUM TO: Investigative Operations Division Personnel
FROM: Angel Gonzalez, 
Acting Assistant Director
SUBJECT: Use of the Investigative Operations Division Shared Drive

During a recent review, it was determined that certain folders and files on the Investigative Operations Division (IOD) shared drive contain Personally Identifiable Information (PII). As you know from both your CSAT training and the Rules of Behavior that each employee must sign, it is critical that any document with PII or potential PII be safeguarded. This includes documents with Social Security Numbers, travel card/purchase card numbers, home addresses and/or phone numbers, passport numbers, performance reviews, contractor pay rates, or any similar document.

In response to this review, we have examined the shared drive and taken steps to identify documents, files, and folders that contain PII. When an owner of the file or folder has been identified, that individual has been contacted and instructed to delete, move, or protect the folder by either locking it down through the USM-169 process, or placing a password on it.

In addition, IOD plans to take further corrective action to ensure that documents containing PII are not accessible to individuals who should not have access to them. Beginning August 1, 2014, all Headquarters Branch Chiefs and Regional Field Chiefs are instructed to oversee a comprehensive review and clean-up of all folders and files that appear on the shared drive. The IOD Records Management Specialist will provide detailed instructions on USMS retention policies that will assist in determining whether files can be deleted or archived. Of course, certain files have historical significance and should be retained either on the shared drive or on SharePoint team sites. Nothing should be deleted that may be useful in a historical context. The Executive Support Staff can assist you in creating team sites and establishing permission levels for files and documents.

Further, IOD is working with the Information Technology Division (ITD) to develop and disseminate Standard Operating Procedures for proper use of the shared drive, which likely will become a model available to the entire Agency. To that end, it is important that all IOD offices,

Memorandum from Acting Assistant Director Gonzalez
Subject: Use of the Investigative Operations Division Shared Drive

Page 2

both at Headquarters and in the field, follow the established division protocol for approving USM-169 forms. All USM-169 forms should be signed by the IOD Administrative Officer, currently Chief Denise Levenberry. Branch Chiefs, Regional Chiefs, and Supervisory Inspectors should not sign and submit USM-169 forms independently.

Safeguarding of PII is an Agency and DOJ priority. I ask that all IOD employees exercise extreme care when posting documents on the share drive to ensure that nothing containing PII or other information of a possibly sensitive nature is universally accessible.

If you have any questions, please contact Chief Inspector Jen Armstrong at 202-305-9405 or via email at Jennifer.Armstrong@usdoj.gov.