U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

The Special Counsel

January 22, 2015

The President
The White House
Washington, D.C. 20510

Re: OSC File No. DI-14-1514

Dear Mr. President:

Pursuant to my duties as Special Counsel, enclosed please find the Department of Justice's report based on disclosures of wrongdoing at the United States Marshals Service (USMS), Investigative Operations Division (IOD), Alexandria, Virginia. OSC has reviewed the report and, in accordance with 5 U.S.C. §1213(e), provides the following summary of the allegations and our findings.

The whistleblower, Mr. James Ergas, a USMS chief inspector, who consented to the release of his name, alleged that agency officials engaged in conduct that may constitute a violation of law, rule, or regulation. Specifically, Mr. Ergas asserted that that IOD employees failed 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 (HIPAA) of 1996, and DOJ orders.

The agency substantiated Mr. Ergas's allegations. The report noted that the investigation confirmed that large amounts of unsecured PII was stored on IOD shared hard drives in violation of the Privacy Act, DOJ orders, and USMS policy directives. The agency did not find evidence of willful or criminal violations of the Privacy Act, and attributed the unsecured information to administrative error. The agency took immediate measures to correct the problem by removing PII from the shared drive and limiting access within the division. In addition, the agency developed a written protocol for the use of shared drives nationally. Based on my review, I have determined that the investigative report contains all the information required by statute and the findings appear to be reasonable.

Mr. Ergas's allegations were referred to Attorney General Eric H. Holder, Jr. to conduct an investigation pursuant to 5 U.S.C. § 1213(c) and (d). Review of the matter was delegated to USMS Director Stacia A. Hylton, who appointed U.S. Marshal James A. Thompson to conduct an investigation. On August 25, 2014, Armando O. Bonilla, associate deputy attorney general, submitted the agency's report to OSC. Pursuant to 5 U.S.C. § 1213(e)(1), Mr. Ergas was given the opportunity to provide comments on the

agency report and did so on November 26, 2014. As required by 5 U.S.C. § 1213(e)(3), I am now transmitting the report to you.[1]

I. Mr. Ergas's Disclosures

Mr. Ergas alleged that the IOD shared drive, which includes thousands of unsecured documents containing PII, was improperly accessible by a large number of current and former USMS operational and administrative personnel, contractors, and staff from other USMS districts and divisions. Mr. Ergas explained that network administrators have the ability to password protect sections of the drive, but did not enable this feature for the majority of folders.

Mr. Ergas examined the contents of the shared drive and discovered that it contained a large number of unprotected files. These files included personal information on individuals who had filed grievances against the agency, and names and Social Security numbers of both current and past employees. It also included similar PII for USMS Task Force officers at the state, local and federal levels, including home address information. In addition, Mr. Ergas discovered files containing birth dates and address information for IOD personnel.

Mr. Ergas also discovered unsecured files containing past and current government travel card numbers, government purchase card numbers, and federal expense account information. Mr. Ergas saw files containing the disposition of IOD disciplinary procedures, including information on punishment recommendations.

Finally, Mr. Ergas found files and forms containing medical information of IOD personnel who were injured in the line of duty. Mr. Ergas explained that the IOD shared drive contains Department of Labor CA-1 and CA-16 forms, which provide notice of traumatic injuries and duty status reports to federal employers. CA-1 forms include health information such as the nature, location, and cause of bodily injuries. CA-17 forms contain sections that must be completed by treating physicians detailing medical diagnoses, clinical findings, and recommendations. These forms also included names, Social Security numbers, home addresses, and dependent information. The contents of

---

[1] The Office of Special Counsel (OSC) is authorized by law to receive disclosures of information from federal employees alleging violations of law, rule, or regulation, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health and safety. 5 U.S.C. § 1213(a) and (b). OSC does not have the authority to investigate a whistleblower's disclosure; rather, if the Special Counsel determines that there is a substantial likelihood that one of the aforementioned conditions exists, she is required to advise the appropriate agency head of her determination, and the agency head is required to conduct an investigation of the allegations and submit a written report. 5 U.S.C. § 1213(c). Upon receipt, the Special Counsel reviews the agency report to determine whether it contains all of the information required by statute and that the findings of the head of the agency appear to be reasonable. 5 U.S.C. § 1213(e)(2). The Special Counsel will determine that the agency's investigative findings and conclusions appear reasonable if they are credible, consistent, and complete based upon the facts in the disclosure, the agency report, and the comments offered by the whistleblower under 5 U.S.C. § 1213(e)(1).

these forms indicate that they are considered protected health information and must be maintained in accordance with HIPAA. Mr. Ergas stated that these forms are not password protected and are stored in a location on the IOD drive where they are easily accessible.

Pursuant to the Privacy Act (the Act), agencies are responsible for establishing appropriate safeguards to protect privacy information. *See* 5 U.S.C. § 552a (e)(10). In accordance with the Act, DOJ Information Technology Security Order 2640.2F (November 26, 2008) was issued for the purpose of "ensuring the confidentiality, integrity, and availability of…systems, networks, and data." This order specifically requires a reduction in the volume of collected and retained PII to necessary minimums, limitations on individual access to such files, and the categorization of sensitive PII and systems processing such information as moderate- or high-impact. Such categorization is intended to assess the potential consequences of an event jeopardizing the security of this information. In addition, DOJ networks must log all computer-readable data extracts from databases holding sensitive information. *See* DOJ 2640.2F §2.10. DOJ orders also broadly define what constitutes a PII breach. For example, a breach occurs when an individual other than an authorized user has access or potential access to information. *See* DOJ Order 2880.IC.

II. The Agency's Report

The report substantiated Mr. Ergas's allegations. The investigation discovered inappropriate maintenance of PII in violation of the Privacy Act, DOJ Orders, and USMS policy directives. In addition, the investigation confirmed that all nine types of unsecured information, which Mr. Ergas asserted existed on the drive, were present and unprotected.

The investigation determined that the shared drive contained 72 folders and 204 documents and spread sheets. Within each of the 72 folders there were numerous subfolders, which contained between one and 218 documents, some dating as far back as 2002. The report provided an illustrative table detailing the type of unsecured information uncovered. For example, the table indicated that the share drive contained unsecured documents including:

- Approximately 2,500 employee names with social security numbers (SSNs)
- Approximately 1,200 employee badge and credentialing numbers, with associated SSNs
- Approximately 1,725 purchase card account numbers, with employee information and SSNs
- Approximately 1,000 employee evaluations plus disciplinary and grievance information
- Folders containing employee medical information and medical clearance evaluations

When IOD managers were interviewed, they were unable to explain why such a wide array of documents was unsecured and available to all IOD personnel. These individuals were likewise unfamiliar with the technical process of securing files. Some officials attributed the problem to a failure to reassign the responsibility for maintaining the shared drive after the retirement of a highly regarded administrative officer. In addition, the investigation noted that IOD is one of the largest divisions in USMS with hundreds of employees with varying lengths of service within the unit. Given these factors, the investigation found that constant monitoring of computer access was required, but user access permissions are frequently ignored when personnel leave the unit. The agency did not find any evidence of willful or criminal violations of the Privacy Act, and attributed the unsecured information to administrative oversight. As a result no disciplinary actions were required.

The report noted that IOD managers took immediate action to resolve the problem when they were alerted to OSC's referral letter. Managers identified documents that required enhanced protection, and began transferring files to secured folders on the shared drive. Old folders with unneeded data were deleted. IOD senior management determined that it was necessary to create new guidelines for data maintenance for all staff, and enlisted the assistance of a records management specialist to ensure that records are properly secured.

In response to this situation, information technology security personnel are developing a USMS-wide protocol for USMS shared drives that will govern the content of data placed on these systems. The report partially attributed the PII issues to frequent staff turnover and movement within USMS and explained that USMS was working toward obtaining a computer program that will facilitate more flexible and effective management of employee access rights and will be capable of responding to these frequent staffing changes. In addition, USMS is implementing an enhanced IT training program, as recommended, to educate employees on how to manage and protect PII. The report also noted that despite the large volume of unsecured data on the shared drive, there was no evidence of misuse of this information, nor were any victims of identity theft identified.

III. The Whistleblower's Comments

Mr. Ergas expressed disappointment with the agency's findings. Specifically, he objected to the fact that no disciplinary action was taken against USMS officials who were responsible for managing the security of the PII at issue. Mr. Ergas further noted that while the report did not find any inappropriate use of financial information contained on USMS shared drives, this does not mean it did not occur, and the agency did not demonstrate it had any way of determining whether unsecured data was accessed in the first place. In addition, Mr. Ergas called attention to the fact that no employees were

notified that their information was compromised, or what type of information was available.

IV. The Special Counsel's Finding

I have reviewed the original disclosure and the agency report. While Mr. Ergas raises valid concerns in his comments particularly the failure to notify employees of the issue, the agency took immediate steps to secure the PII at issue, developed a protocol to govern content placed on shared drives, and implemented a training program to prevent these issues from happening in the future. The investigation also determined that there was no evidence suggesting that PII was accessed and disclosed improperly. For these reasons, I have determined that the findings of the agency head appear reasonable and the agency report meets all statutory requirements.

As required by 5 U.S.C §1213(e)(3), I have sent copies of the agency report and the whistleblower's comments to the Chairmen and Ranking Members of the Senate and House Judiciary Committees. I have also filed copies of the agency reports and the whistleblower's comments in OSC's public file, which is available online at www.osc.gov. This matter is now closed.

Respectfully,

Carolyn Lerner

Carolyn N. Lerner

Enclosures