



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

The Special Counsel

June 7, 2016

The President
The White House
Washington, D.C. 20500

Re: OSC File No. DI-15-4560

Dear Mr. President:

Pursuant to my duties as Special Counsel, I am forwarding a Department of Justice (DoJ) report based on disclosures of wrongdoing at the DoJ, U.S. Marshals Service (USMS), Tactical Operations Division (TOD), Arlington, Virginia. I have reviewed the report and whistleblower comments, and in accordance with 5 U.S.C. § 1213(e), provide the following summary of the agency report, and my findings.¹

The whistleblower, who chose to remain confidential, alleged that TOD employees failed to follow appropriate procedures for safeguarding and disposing of personally identifiable information (PII) in violation of the Privacy Act of 1974 and DoJ orders. I referred the whistleblower's allegations to Attorney General Loretta E. Lynch for investigation pursuant to 5 U.S.C. § 1213 (c) and (d). Investigation of the matter was delegated to the USMS Office of Professional Responsibility. Associate Deputy Attorney General Raphael A. Prober was delegated the authority to review and sign the report. On December 3, 2015, Mr. Prober submitted the agency's report to the Office of Special Counsel (OSC). The whistleblower provided comments on February 29, 2016. On May 25, 2016, Mr. Prober submitted additional information concerning a risk assessment conducted into the matter.

The agency substantiated the whistleblower's allegations, finding that PII was not appropriately protected on TOD shared drives. In response to this finding, TOD took immediate steps to archive or remove PII from shared drives, limit or restrict access to PII, and actively engaged with the USMS Information Technology Division to implement

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).

The Special Counsel

The President
June 7, 2016
Page 2 of 2

training and protocols for managing PII. In addition, the agency developed a plan to protect PII within the agency, and purchased a scanning tool that will routinely search for PII not contained in protected folders. Under agency procedures, DoJ's Computer Emergency Readiness Team and Department Security Officer were notified, and they conducted a risk assessment to determine the appropriateness of employee notification. The assessment, which was completed in March 2016, indicated that there was no evidence that any vulnerable information was used to commit identity theft, and there was no general knowledge of the accessibility, or any known instances of misuse or unauthorized use. As such, no employee notification was warranted.

The whistleblower's comments called attention to the absence of any mention of accountability or disciplinary action in the report and questioned the investigators' purported inability to determine who accessed the information. The whistleblower called on the agency to provide notification to individuals whose PII was potentially compromised and asserted that this sensitive information could be used against employees in a variety of ways.

I have reviewed the original disclosure, the agency report, and the whistleblower's comments. The whistleblower raised serious and valid concerns regarding the lack of accountability and notification in this matter. However, after implementing a variety of corrective actions, the agency conducted a comprehensive risk assessment that did not find any evidence suggesting identify theft occurred. For these reasons, I have determined that the report meets all statutory requirements and the findings appear reasonable.

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

Respectfully,



Carolyn N. Lerner

Enclosures