[redacted]

February 11, 2024

[redacted]
U.S. Office of Special Counsel
1730 M Street NW, Suite 218
Washington, DC 20036-4505

SUBJECT: OSC File No. DI-22-000680
Whistleblower Comments

Dear [redacted]:

I am writing to provide comment on a November 6, 2023 supplemental report by the U.S. Department of Veterans Affairs (VA) concerning OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742.

Analysis of VA's Response to OSC Question 1

VA's response to OSC question 1 is not just disappointing—**it is an egregious display of negligence, evasion, and a fundamental disregard for proper procedure and accountability**. Remember that OSC referred this case to VA Secretary Denis R. McDonough for investigation and report on or about August 2, 2022. At that time, the lax security conditions and general mismanagement of VIEWS met the criteria for a "data breach" pursuant to VA Handbook 6500.2. However, 332 days later (on June 30, 2023), VA published a new version of VA Handbook 6500.2 that redefined "data breach" such that the disastrous VIEWS situation no longer qualified as a breach. Just 21 days later (on July 21, 2023), VA issued a report back to OSC asserting that no breech took place based on the new definition in VA Handbook 6500.2.

Considering that this new definition (1) was issued just 21 days before VA published its July 21, 2023 report to OSC, and (2) specifically allows for the type of "incidental" access to PII and PHI that VA alleges in its July 21, 2023 report to represent the extent of access that occurred due to VIEWS system security failures, raises serious doubts as to the ethicality of this redefinition and indicates a concerted, coordinated effort by VA executives to protect themselves and VA given the seriousness of our allegations. Even more concerning is that this VA policy change appears to be in violation of the Privacy Act, which does not allow agencies to evade responsibility for "incidental" disclosures of sensitive personal records.

VA's assertion that it is appropriate to change a policy after the Department is caught with its pants down and directed to investigate the matter is an insult to the intelligence of Congress, the President, and the American public. In fact, in this case, VA's attempt to absolve itself of wrongdoing has backfired: while the new version of VA Handbook 6500.2 redefines "data breach," the handbook does *not* indicate that the new definition applies retroactively. Therefore, VA must apply the former definition to data security incidents that pre-date the revised "data breach" definition. The fact remains that during the timeframe of

the allegations and the investigation, the 2019 version of the handbook was the operative policy. Ignoring this fact demonstrates a flagrant disregard for protocol and undermines the integrity of the investigation process.

Furthermore, VA's attempt to justify its decision by claiming that the 2019 definition of breach is somehow "obsolete" and "inferior" is nothing short of absurd. The 2019 definition, which clearly defines a breach as the potential acquisition, access, use, or disclosure of sensitive personal information in a manner not permitted by law or policy, is perfectly clear and applicable to the situation at hand. By cherry-picking definitions to suit its narrative, VA is manipulating the facts to absolve itself of any wrongdoing, all while undermining the credibility of its own investigation.

Additionally, VA's reliance on "common parlance" to interpret the term "privacy breach" is a laughable attempt to sidestep accountability. The fact that the handbook's definition of breach aligns with common understanding does not excuse VA from adhering to its own policies and procedures. By dismissing the handbook definition as "inapplicable," VA is effectively rendering its own policies meaningless and opening the door to further confusion and inconsistency in future investigations.

Finally, VA's assertion that there is no breach when the probability of compromise is low is not only nonsensical but also dangerously negligent. The very purpose of defining a breach is to establish clear parameters for identifying and addressing security incidents, regardless of the perceived probability of compromise. By downplaying the significance of potential breaches, VA is failing in its duty to protect sensitive information and uphold the trust of the individuals it serves.

In conclusion, VA's response to the OSC question is not only deeply unsatisfactory but also indicative of a broader pattern of incompetence and irresponsibility within the Department. If VA is truly committed to serving the best interests of the public, it must take immediate steps to rectify this situation, hold those responsible accountable, and restore confidence in its ability to fulfill its obligations effectively and ethically. Anything less would be a betrayal of the trust placed in it by the American people.

Analysis of VA Response to OSC Question 2

VA's response to OSC Question 2 is nothing short of an abdication of responsibility and a glaring example of the Department's failure to prioritize accountability and the protection of sensitive personal information of Veterans and employees.

Firstly, VA's assertion that it has focused its efforts on improving the VIEWS CCM system to protect sensitive personal information is utterly insufficient in addressing the issue at hand. While implementing changes to designate certain cases as "Sensitive" may be a step in the right direction, it does not excuse the lack of accountability for past violations. VA's attempt to sidestep the question of holding users accountable for incorrectly opened cases is a clear indication of its disregard for the severity of the situation.

Furthermore, VA's justification for not pursuing accountability for past violations is deeply flawed. The argument that attempting to determine past users who improperly opened cases would involve significant manpower and may not be feasible is a feeble excuse for inaction. The fact that mistakes may have been attributable to inadequate training and inadvertent errors does not absolve VA of its duty to investigate and address breaches of protocol. By failing to hold individuals accountable for their actions, VA is sending a dangerous message that negligence and incompetence will be tolerated.

Moreover, VA's proposed solution of implementing a monthly audit program to ensure accountability moving forward is insufficient to address the systemic issues within the Department. While auditing new cases may help prevent future violations, it does nothing to address the lack of accountability for past infractions. Additionally, the vague promise of applying a "progressive discipline approach" to individuals incorrectly opening cases without proper sensitivity is meaningless without concrete measures in place to enforce it.

In conclusion, VA's response to OSC Question 2 is a grossly inadequate attempt to deflect from its failure to uphold accountability and protect sensitive personal information. The Department's unwillingness to hold individuals accountable for past violations is a betrayal of the trust placed in it by the American people and undermines the integrity of its mission. It is imperative that VA take immediate and decisive action to rectify this situation and restore confidence in its ability to safeguard sensitive information effectively and ethically.

Analysis of VA Response to OSC Question 3

VA's response to OSC Question 3 is not only disappointing but also deeply concerning, as it reveals a blatant disregard for transparency and accountability.

VA's attempt to justify withholding the key that identifies employees by name and position by citing concerns about "leaks" to the media is disingenuous, unacceptable, and downright hypocritical. This entire case is about VA's years-long failure to safeguard highly sensitive personal information of Veterans and employees. Only now that VA is in the hot seat for this security failure is the Department suddenly concerned with protecting the identity of those responsible.

Upon review of the witness list, it was disappointing to learn that VA failed to interview the current Deputy Secretary, who has been caught providing perjurious testimony to the U.S. Senate Committee on Veterans' Affairs concerning the instant case.

By prioritizing its own interests over the need for transparency and accountability, VA has undermined the integrity of its investigative process and has further eroded public trust in the Department.

Analysis of VA Response to OSC Question 4

VA's response to OSC Question 4 is a testament to its systemic failures and its complete disregard for accountability and transparency. The timeline provided

by VA is riddled with delays, incomplete actions, and a shocking lack of urgency in addressing critical issues surrounding the protection of sensitive personal information.

Firstly, while VA claims to have completed certain recommended corrective actions, it fails to provide evidence of their effectiveness or any tangible outcomes. Merely stating completion dates without demonstrating the impact of these actions is insufficient and raises serious doubts about VA's commitment to addressing the underlying problems identified in the report.

Furthermore, VA's timeline for completing the remaining recommended corrective actions is woefully inadequate. Many of the actions are slated for completion in future fiscal years, suggesting a lack of urgency in addressing pressing concerns. Delaying action on critical security measures leaves sensitive personal information vulnerable to exploitation and undermines the trust of the individuals whose data VA is entrusted to protect.

Additionally, VA's response is characterized by a disturbing lack of accountability. Instead of taking ownership of the issues outlined in the report, VA deflects responsibility by citing concerns about leaks to the media and proposing cumbersome review processes. This evasion of accountability further erodes trust in VA's ability to effectively address the challenges it faces.

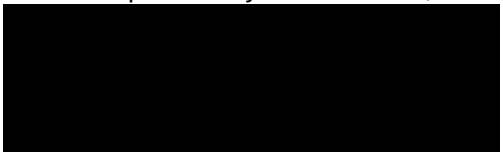
In conclusion, VA's response to OSC Question 4 is a grossly inadequate attempt to address serious deficiencies in its handling of sensitive personal information. The timeline provided is marked by delays, incomplete actions, and a disturbing lack of accountability. It is imperative that VA take immediate and decisive action to rectify these shortcomings and restore confidence in its ability to safeguard the privacy and security of the individuals it serves.

CONCLUSION

VA's responses to OSC's four questions demonstrate a continued pattern of negligence, evasion, and a fundamental disregard for accountability and transparency that necessitate aggressive action and intervention by the President and Congress. VA's attempts to deflect responsibility, manipulate definitions, and prioritize the interests of its executives over those of the individuals it serves are deeply concerning and indicative of systemic failures throughout the Department. From redefining terms to suit its narrative to failing to hold individuals accountable for past violations, VA's responses fall short of the standards expected of a government agency entrusted with safeguarding sensitive personal information. It is imperative that VA takes immediate and meaningful action to address these deficiencies, restore public trust, and fulfill its obligations effectively and ethically. Anything less would be a disservice to the American people and a betrayal of the trust placed in the Department.

Thank you for providing this opportunity to respond to VA's report.

Respectfully submitted,



[redacted]