[redacted]

September 4, 2023

[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 July 21, 2023 "Report to the Office of Special Counsel" by the U.S. Department of Veterans Affairs (VA) concerning OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742.

In late June 2022, while still employed by VA, two colleagues and I each filed separate whistleblower disclosures to the U.S. Office of Special Counsel (OSC) alleging that VA officials are violating the Privacy Act of 1974 and the provisions of VA Directive 6502 and VA Handbook 6500 by improperly storing the personally identifiable information of whistleblowers, employees, and veterans in the Veterans Affairs Integrated Enterprise Workflow Solution (VIEWS) system of records because such sensitive information is not marked as sensitive and is therefore accessible to all VA employees that have access to VIEWS.

After reviewing the evidence that my colleagues and I provided, OSC determined that there is a substantial likelihood of wrongdoing by VA. OSC subsequently referred the disclosures to VA Secretary Denis R. McDonough for investigation and report on or about August 2, 2022. It was not until July 21, 2023—**353 days later**—that VA finally issued its report to OSC. However, far more troubling is what VA officials did in that time period to evade culpability.

What follows is my analysis of VA's July 21, 2023 report, which begins with my feedback on the report, followed by three additional recommendations for VA, and ends with three new allegations of wrongdoing by VA resulting from this investigation.

REPORT FEEDBACK

I would like to begin by thanking the investigator assigned to this case. I found him to be a consummate professional in all of my interactions.

Role of VA Office of Information & Technology (OIT): Aside from the shamelessly misleading Executive Summary, the body of VA's July 21, 2023 report captures the myriad of very serious and consequential missteps by VA and Salesforce regarding the security of sensitive personal information. What I find most interesting is the role of OIT and the fact that this particular office was asked to investigate considering that the VIEWS system was created and is maintained

pursuant to a contract with Salesforce that is managed through OIT. As effective as the investigator might have been, this arrangement creates the appearance of an ethical conflict and should have been avoided.

Data Breach: Page 17 of the report states, "It should be emphasized that there is no evidence that VIEWS vulnerabilities discussed in this report resulted in a privacy breach or has caused harm to Veterans, whistleblowers, or their families." This finding is in error. Simply, the instant investigation did not examine privacy breaches and the harm caused to Veterans, whistleblowers, and their families due to VIEWS' security flaws—the assigned investigator is without the capacity, authority, training, and jurisdiction required to conduct such an investigation. Thus, VA has no basis to assert that there exists no evidence of a privacy breach or resulting harm.

Countless whistleblowers have come forward alleging otherwise unexplainable acts of retaliation, theft, vandalism, threats, and physical harm after blowing the whistle—VIEWS may very well be the source of information that fueled these illegal acts, but not until that is investigated properly will we know for certain.

Freedom of Information Act (FOIA) & Privacy Act Requests: VA claims it was "unable to substantiate" Allegation 3, which asserts that "VA officials have failed to include VIEWS in FOIA and Privacy Act requests, in violation of federal law and agency directive and handbook provisions." This finding is invalid and should be changed to "Substantiated."

First, consider that the report notes that VA's FOIA Office pointed to only three instances in which VIEWS was searched for responsive documents even though VA processes many thousands of FOIA and Privacy Act requests annually.

Second, consider that in a FOIA request dated August 6, 2021, from [redacted] of Empower Oversight, VA was asked to provide "all records relating to … [the VA's] receipt of, discussions related to, processing of, and response to Senator Grassley's April 2, 2021 letter to Secretary McDonough and/or his July 20, 2021 letter to Secretary McDonough." VA's response to this FOIA request failed to include responsive documents housed in VIEWS. I know this because I personally saw those records in VIEWS while employed at VA and have since come to learn that VA did not include them in its response to [redacted].

Therefore, it can be substantiated that VA officials have failed to include VIEWS in FOIA and Privacy Act requests, in violation of federal law and agency directive and handbook provisions. Further, the fact that VA does not track Privacy Act requests globally is not a reason for VA not to examine this component of the allegation—this must be investigated broadly, as different VA offices may apply different practices.

ADDITIONAL RECOMMENDATIONS

Recommendation 1: *Notify and provide credit protection services to those whose sensitive personal information was marked "not sensitive" in VIEWS.*

Given VA and Salesforce's years-long failure to secure sensitive personal information housed in the VIEWS system, the PII and PHI of potentially millions of Veterans and VA employees have long been freely available for the taking.

And no amount of training or annual affirmation of VA privacy policy by VIEWS users is going to prevent a bad actor from victimizing any of these individuals. As such, VA should be obligated to notify and provide identity theft protection to all Veterans and employees whose sensitive personal information was left exposed in VIEWS for any length of time. Through this report, VA has lost credibility with Veterans and employees, and restoring that trust involves more than fixing VIEWS—it requires the protection of those whose trust VA violated by making their PII and PHI available for more than 2,000 VA employees and contractors to see.

Recommendation 2: *Reopen and revisit all whistleblower cases cited in VIEWS.*

As a whistleblower myself, I am especially troubled by the report's acknowledgement that "many thousands of [VIEWS cases] containing detailed information about VA employee whistleblower retaliation complaints [were] potentially accessible to the very people who were alleged to have committed wrongdoing" (p. 10). This conclusion alone obligates VA, OSC, and the U.S. Merit Systems Protection Board (MSPB) to reopen every whistleblower case referenced in VIEWS that was closed because the whistleblower was unable to prove that the retaliator had prior knowledge of the whistleblower's protected activity.

Recommendation 3: *Demand that Salesforce fix the security vulnerabilities of VIEWS at no additional cost.*

On pages iv, v, 18, and 19, there are recommendations for VA to acquire "Einstein Data Detect," a Salesforce product, to help protect privacy in VIEWS. It is difficult to understand why VA would pay Salesforce more money to acquire another Salesforce product to fix the security vulnerabilities of an existing Salesforce system (i.e., VIEWS). VA should enforce the terms of the existing contract and demand that Salesforce correct the problem at no further cost to the American taxpayer.

NEW ALLEGATIONS OF WRONGDOING BY VA

New Allegation 1: *In its July 21, 2023 report, VA improperly used a three-week-old version of VA Handbook 6500.2 to draw findings on certain allegations from OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742, which was not the version of VA Handbook 6500.2 in effect in August 2022 when OSC directed VA to investigate and report on the same allegations.*

The conditions that led to the allegations of wrongdoing cited in OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742 existed when VA Handbook 6500.2 (March 12, 2019) was in effect. Further, that same handbook was in effect for nearly 11 months after OSC directed VA to investigate the allegations. However, in what can only be described as an eleventh hour switcheroo, VA brazenly replaced the contents of VA Handbook 6500.2 with a new version that coincidentally limits its liability in data security situations precisely like those that impacted the VIEWS system and disingenuously cited the revised VA Handbook 6500.2 language in its July 21, 2023 report without referencing its June 30, 2023 publication date or mentioning that an earlier version was in effect when OSC issued its order to investigate.

That VA evaluated the subject allegations in accordance with the three-week-old version of VA Handbook 6500.2, and not the one that was in place when the allegations were made, is wrong and should not be permitted. If left uncorrected, such would enable any agency or office accused of violating its own policies to modify said policies during an investigation to evade all liability. The consequences could be devastating to our nation.

New Allegation 2: *VA executives conspired to delay publication of VA's July 21, 2023 report to OSC and to modify VA Handbook 6500.2 to limit the possible findings of wrongdoing and recommended corrective actions in response to OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742.*

VA was originally granted 60 days to respond to OSC's demand for an investigation and report. However, VA repeatedly requested time extensions while it cobbled together a half-hearted solution in time for the report's release. We also learned that VA bought time to water down the report's language and even modify internal policy to soften the blow of the findings. All told, VA's original 60-day turnaround period turned into a 353-day charade.

On June 30, 2023, VA's Assistant Secretary for Information Technology published a revised version of VA Handbook 6500.2 ("Management of Breaches Involving Sensitive Personal Information"), which redefined the term "breach" such that VA's failure to properly secure PII and PHI in its VIEWS system no longer qualifies as a "breach." The most recent past version of VA Handbook 6500.2, dated March 12, 2019, defined the term "breach" as:

> *The potential acquisition, access, use, or disclosure of VA sensitive personal information in a manner not permitted by law or VA policy which compromises the security or privacy of that information.*

However, the new version defines "breach" as:

> *A loss or theft of, or other unauthorized access to, other than an unauthorized access incidental to the scope of employment, data containing [sensitive personal information], in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.*

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.

New Allegation 3: *VA's new version of VA Handbook 6500.2, dated June 30, 2023, includes a revised definition of "breach" (vs. the definition in the previous version of VA Handbook 6500.2, dated March 12, 2019), such that it violates the 'need to know' provision of the Privacy Act (5 U.S.C. § 552a(b)(1)).*

The Privacy Act states:

> *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains unless the disclosure would be [...] to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.* 5 U.S.C. § 552a(b)(1)

Each time one of VA's 2,000+ VIEWS system users accessed Veteran and Whistleblower PII and PHI through VIEWS, VA effectively *disclosed* that PII and PHI to the VIEWS system user. When that that disclosure is for a legitimate business purpose—for example, the disclosure of a Veteran's social security number through the VIEWS system so the VIEWS system user could track down a separate record on behalf of the subject Veteran—there exists an obvious "need to know" and thus, no violation of the Privacy Act. However, when that disclosure is unintentional or without a legitimate business purpose—such as when an unrelated VIEWS system user accesses the protected disclosures of a Whistleblower in VIEWS or when a VIEWS system user downloads and views the wrong Veteran's DD-214—there exists no "need to know."

Courts generally have found that intra-agency disclosures to employees that do not have a need for a given record in the performance of their duties are outside the scope of the "need to know" disclosure exception. Thus, by effectively allowing "incidental" disclosures of PII and PHI to employees who do not have a "need to know," pursuant to the latest version of VA Handbook 6500.2, VA is operating in violation of the Privacy Act, which requires a "need to know" and provides no exceptions for "incidental" disclosures.

CONCLUSION

The mishandling of sensitive personal information occurred for three reasons. First, certain users were knowingly or inadvertently negligent in applying proper sensitivity thresholds to VIEWS system cases containing the PII and PHI of Veterans and VA employees despite VA security policy prohibiting such activity. Second, no technical controls were in place to prevent negligent users from failing to protect VIEWS system cases containing PII and PHI. Third, due to a lack of oversight, the VA Chief of Staff, VA Executive Secretariat, and OIT personnel failed to discover and secure sensitive personal information marked as "not sensitive" in VIEWS.

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

Respectfully submitted,

[redacted]