DEPARTMENT OF VETERANS AFFAIRS
Washington, DC
Report to the Office of Special Counsel
OSC File Number Dl-22-000682

Re: Statement of [redacted] OSC File No. Dl-22-000682-February 11, 2024

Comments in response to a copy of the supplemental report (herein "Report") the U.S. Office of Special Counsel (OSC) received from the Department of Veteran Affairs (VA) in response to allegations that employees at the VA, Washington, D.C., engaged in conduct that may constitute a violation of law, rule, or regulation.

Comments to VA's Response to OSC's Question#1:

The VA stated in their response to Question #1 in the Supplemental OSC Report "Finally, as a general principle, an agency is obligated "to apply the law in effect at the time it renders its decision, unless doing so would result in manifest injustice or there is statutory direction or legislative history to the contrary."

The Agency rendered it's decision in May 2023. On May 30, 2023, the investigator stated to the whistleblower "My report is mostly complete though – just going through some final steps." One month later, June 30, 2023, the VA changed the definition of the word "data breach," to a definiton inconsistent with the definition of data breach in the CFR. The June 30th revised definition of the word "data breach" in the VA Handbook is in conflict with the CFR and therefore there is "statutory direction or legislative history to the contrary". The 2019 VA Handbook definition of data breach that was current at the time of the VA's decision (May 2023) was consistent with the CFR.

The multi-thousands of documents (confirmed by the VA's Initial Report to OSC) in VIEWS not marked sensitive and visible to any user resulting in the potential compromise of
the confidentiality or integrity of the data is in fact a data breach and to call it otherwise would result in a "manifest injustice" as the victims have no rights to credit counseling and/or other legal remedies afforded to them in the event of a data breach. The application of the 2019 policy would change the VA's report findings and conclusions. The probability of the information compromised is not low. One document of one whistleblower showed 19 downloads prior to VA canceling the auditing software for VIEWS. There are over 3.6 Million documents in VIEWS and the documents not marked sensitive were in the multi-thousands.

38 CFR § 75.113 - Data breach

Consistent with the definition of data breach in § 75.112 of this subpart, a data breach occurs under this subpart if there is 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. The term "unauthorized access" used in the definition of "data breach" includes access to an electronic information system and includes, but is not limited to, viewing, obtaining, or using data

containing sensitive personal information in any form or in any VA information system. The phrase "unauthorized access incidental to the scope of employment" includes instances when employees of contractors and other entities need access to VA sensitive information in order to perform a contract or agreement with VA but incidentally obtain access to other VA sensitive information. Accordingly, an unauthorized access, other than an unauthorized access incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data, constitutes a data breach. In addition to these circumstances, VA also interprets data breach to include circumstances in which a user misuses sensitive personal information to which he or she has authorized access.

Unauthorized access incidental to the scope of employment means access, in accordance with VA data security and confidentiality policies and practices, that is a by-product or result of a permitted use of the data, that is inadvertent and cannot reasonably be prevented, and that is limited in nature.

The VIEWS data breach was not inadvertent (VA used sensitive controls for other documents but disregarded the controls for whistleblower documents and documents that contain pii and personal information), and it can reasonably be prevented by using the controls provided (sensitive button). The unauthorized access to the records was not limited in nature. The report found that based on the number of cases that users incorrectly opened in VIEWS CCM as Not Sensitive-estimated at multi-thousands.

Comments to VA's Response to OSC's Question#2:

The VA stated "because of the scale and labor-intensive nature of any such project, attempting to determine past users who improperly opened cases would likely involve many hundreds, if not thousands, of man-hours. It also is not clear whether such a project would be feasible given the significant recent changes to the system. In addition, many of these mistakes in opening VIEWS cases without the proper sensitivity may have been attributable to inadequate training and inadvertent errors. As a result, VA does not believe such an effort to review past cases, to identify users who incorrectly opened VIEWS cases would be an effective allocation of resources."

P.L. 109-461 requires that in the event of a "data breach" of sensitive personal information processed or maintained by the VA Secretary, the Secretary must ensure that as soon as possible after discovery that either a non-VA entity or the VA's Inspector General conduct an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information. Based upon the risk analysis, if the Secretary determines that a reasonable risk exists of the potential misuse of sensitive personal information, the Secretary must provide credit protection services in accordance with regulations issued by the VA Secretary. This law does not mention allocation of resources and/or thousands of man hours to determine the extent of the data breach as a bar to accountability.

The Privacy Act of 1974 provides that if any officer or employee of a government agency knowingly and willfully discloses personally identifiable information will be found guilty of a misdemeanor and fined a maximum of $5,000. Also, if any agency employee or official willfully maintains a system of records without disclosing its existence and relevant details as specified above can be fined a maximum of

$5,000. It is not legal to turn a blind eye on a data breach and fail to hold violators criminally responsible by neglecting to investigate possible criminal activity of employees.

Whistleblowers have rights under the Whistleblower Protection Act and whistleblower's rights have been violated in the VIEWS data breach. Whistleblowers have a right to know who viewed their confidential communications without a need to know, to exercise their rights under the Act.

Furthermore, the VIEWS Privacy Impact Assessment states "All system access is logged, including access to PII. Users of the system (VA employees and contractors) are individually responsible for appropriate system usage. Misuse of information may result in employment termination or legal or civil penalties, as appropriate by law. Additionally, audits are performed to ensure information is accessed and retrieved appropriately." VA Directive 6508 states on page 14 " Privacy Impact Assessment (PIA). A PIA is an analysis that seeks to identify and mitigate the privacy and security risks associated with the use of PII by a program, system, or practice. A PIA provides a framework for examining whether privacy, security and other vital data issues have been identified, addressed, and incorporated into the plan, design, operation, maintenance, and disposal of electronic information systems. PIAs are required to be performed in the conceptualization phase of the system lifecycle and updated whenever a system change could create a new privacy risk." See page 14 of Directive 6508. If VA states they have no auditing tool to determine unauthorized access, the PIA is not accurate and the lack of the security tool creates additional privacy risks. The VIEWS PIA specifically states that misuse of information may result in employment termination or legal or civil penalties, as appropriate by law. Accountability is not ensured by moving forward. VA should be required to perform audits on the system in compliance with the myriad of laws that are supposed to protect an employee from this type of data breach for every occurrence to determine the extent of the unauthorized access and remediation processes.

I do not agree that the Va's answers to the Special Counsel's questions are reasonable.

2/11/2024

[redacted]

[5/30/23 1:45 PM] [redacted] VBACO

HI [redacted] - any update on if my stuff is out of there or marked sensitive?

[5/30/23 1:47 PM] [redacted] VBACO

I did not get too far w the privacy lady...not sure where else to report it

[5/30/23 1:49 PM] [redacted] VBACO

in 25 days it's one year since reporting it I am so frustrated not at you at the process or non process!

[5/30/23 1:50 PM] [redacted]

Sorry - no update. My report is mostly complete though - just going through some final steps.

[5/30/23 1:53 PM] [redacted] VBACO

oh awesome so when will I see it?

[5/30/23 1:57 PM] [redacted]

wish I could say for sure

[5/30/23 2:00 PM] [redacted] VBACO

ok thank you

[redacted] Chat Files 2 more +

1

May 30, 2023

5/30/23 1:45 PM

HI [redacted] any update on if my stuff is out of there or marked sensitive?

I did not get too far w the privacy lady...not sure where else to report it

in 25 days it's one year since reporting it I am so frustrated not at you at the process or non process!

[redacted] 5/30/23 1:50 PM

[redacted] Sorry - no update. My report is mostly complete though - just going through some final steps.

5/30/23 1:53 PM

oh awesome so when will I see it?

[redacted] 5/30/23 1:57 PM

[redacted] wish I could say for sure

5/30/23 2:00 PM

ok thank you