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-August 23, 2023

Comments in response to a copy of the 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.

I. Comments to Key Findings and Conclusions

1. **VA Directive 6502 Definition:** VA Directive 6502 defines a system of records as a collection of records under agency control, from which data is retrieved using personal identifiers such as names or symbols.

2. **Role of VA Chief of Staff:** the VA Chief of Staff has oversight of VIEWS CCM and directed VA OIT to investigate data breach allegations. OIT is tasked with ensuring VA's compliance with the Privacy Act and IT system requirements, particularly those raised in complaints about VIEWS CCM. "The Department of Veterans Affairs (VA) correspondence management is under the authority of the VA Chief of Staff."[1]

3. **Potential Legal Violations:** A report produced by OIT, in conjunction with admissions made by the Chief of Staff in a memorandum dated July 11, 2023, indicates possible violations of criminal and civil laws, as well as breaches of both OMB and VA policies concerning the maintenance of sensitive personal records including PII and PHI.

4. **Historical Context:** The VIEWS system, developed by Salesforce.com, was initiated sometime in 2018 through the White House Veterans Hotline. Since 2019, there have been concerns raised about its privacy measures to OGC and internal investigations concerning confidential records.

5. **SORN Concerns:** System of Records Notices (SORN) are mandated whenever a federal agency maintains and retrieves personal data.[2] Significant changes to a SORN necessitate an amended SORN publication in the Federal Register for notice and comment.[3] The VA adopted VIEWS in 2018, marking significant changes from the 2009 SORN. However, an amended SORN was only published in 2022 — an apparent violation of the Privacy Act.

6. **Legal Implications:** The Privacy Act makes it a misdemeanor, punishable by a fine up to $5,000, for any federal officer to willfully maintain a system of records without providing the required

[1] See RFP, https://sam.gov/opp/309b11fe7f7246fe8de9d2156a9523e7/view, PWS_VIEWS.docx.
[2] 5 USC 552a(e)(4); 5 USC 552a(5); see OMB Circular A-130, Appendix I, 4(c).
[3] VA Handbook 6300.5, published August 3, 2015, page 7-8. Also see OMB guide on SORNs: https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf

notice, and there are no exceptions to this rule.[4] Willful or intentional violations of the Privacy Act may result liability for damages and attorney fees for victims. 5 U.S.C. § 552a(g)(4).

7. **General Observation:** Over the past decade, the VA has shown inconsistencies in upholding transparency and security for sensitive personal data, causing concerns for American taxpayers.

Recommendation: To ensure security and uphold the Privacy Act, Congress should mandate a third-party audit of VA systems, especially VIEWS CCM, and other systems transitioned in the past 5 years where appropriate PTA, PIA, and SORN protocols may not have been followed. The purpose of the audit is to identify and minimize risks, data breaches and/or incidents and enforce the agency's adherence to its regulations and policies.

II. Failure to Disclose Scope Of Violations of Privacy Act Laws

VA acknowledged adopting a new IT system from Salesforce called VIEWS in 2018 that contained PII and PHI of Veterans, whistleblowers, and others. The vendor, Liberty IT Solutions (herein "Liberty"), published in 2018 that VIEWS was implemented in 2017 for the White House Veterans Hotline, and Liberty indicated a "System of Record (SORN) [was] underway."[5] VA elected to not produce a proper amended SORN until 2022.

The Report asserts, on page 15, "Neither a Privacy Threshold Analysis (PTA) nor a Privacy Impact Assessment were required or completed in preparation of VIEWS CCM going live in 2018," without evidence explaining why a PTA or PIA were not required. According to VA Handbook 6508.1, completion of a PTA is required for systems that collects PII. If the PTA finds PII is collected, a PIA must then be performed to evaluate whether a new or amended SORN must be completed. If an amended SORN is required, it must be completed and published to the Federal Register for notice and comment prior to use. VA policy demonstrates a PTA must be performed every year by the System Owner, at a minimum. "The System Owner is responsible for completing the Standard PTA and coordinating with other relevant stakeholders such as the Privacy Officer."[6]

The Report attempted to minimize the Authority to Operate (ATO) requirement error in 2020 by minimizing the error to misclassification of the system as a "minor application" on page 15. However, regardless of whether an ATO was needed, VA was still required to timely complete the PTA prior to operationalizing VIEWS but failed to follow the necessary VA Handbook 6508.1 pages 5-9, in effect since publication, July 30, 2015. However, even the PIA being performed is likely not properly addressed due to a lack of auditing tools from an unexplained data tool change noted in the Report on page 14.

In her July 11, 2023 memorandum, the COS insinuated the agency followed PTA and PIA reporting protocol "appropriate for sensitive information," but that is misleading. In her QFR to Senator Blackburn, the COS stated, VIEWS "is a system implemented in 2018 to replace older processes and tools."[7] Starting in 2017, according to Liberty IT Solutions, VA used VIEWS for its correspondence

[4] VA Handbook 6500.4, published August 19, 2013, page 13
[5] Liberty IT Solutions flyer. Last visited 08/12/2023.
https://appexchange.salesforce.com/partners/servlet/servlet.FileDownload?file=00P3A00000iHXXiUAO
[6] VA Directive 6508, pg 6, version dated 10/15/2014.
[7] QFR, Senator Blackburn, page 4.

including the White House Veterans Hotline. On June 25, 2021, VA published notice of its 2018 decision to rescind the SORN for ExecVA, which was "a repository for Veterans' calls."[8] That system "was migrated along with its records to SalesForce.com," on September 28, 2018. "The SORN covering that information is 75VA001B," now called VIEWS CCM. Privacy concerns were noted in the Report as early as 2019, and given the rescinded ExecVA SORN, VA officials knew or should have known a SORN was required for VIEWS well before 2022. VA Handbook 6300.5 instructs, a significant change requiring an amended SORN includes, "A change that modifies the scope of the system. For example, the combining of two or more existing systems of records."[9] In 2018, VA combined 141VA005Q3 and 75VA001B.

According to the Report on page 15, the 2022 VIEWS CCM SORN, named Case and Correspondence Management (CCM) (not "VIEWS CCM"), was materially deficient.[10] The Report confirms VA falsely stated users would be limited from accessing sensitive personal information unless for official duties. In the newest SORN, VA haphazardly stated, "Records are also maintained in VIEWS," with no explanation as to what "VIEWS" is much less that Salesforce was the vendor for the system.

Additionally, VA no longer apparently possesses VIEWS' original assessments and approval records. See Report, page 15. VA only searched the Enterprise Mission Assurance Support Service (eMASS) without searching other VA systems for these key documents that should have been completed in 2017 or earlier.

The OIT investigator apparently requested logs for audit reports to verify claims of whistleblower data being illicitly accessed, but an undisclosed DTC solution "transition" to a "new data tool" impacted VA's ability to produce usable audit reports. See Report, page 14. No evidence was provided to substantiate why a data tool change prevented completion of the audit.

As a consequence of the unfortunately timed data tool change, like the lack of original assessments and approvals in eMASS, "it is unclear how business and system owners are able to accomplish risk mitigations in the form of auditing user activity as stated in the system's Privacy Impact Assessment (PIA)." See page 14.

III. Report Deflects Responsibility Away From the Chief of Staff's Office

The Report seems to deflect responsibility away from the Chief of Staff's office, and puts all the responsibility on the Executive Secretary and designated Privacy Officer, and Information System Security Officer.

Internal VA documents, including the PWS for the VIEWS contract, cite the COS as having authority over the VIEWS system.[11] The COS also accepted responsibility for decisions regarding VIEWS in correspondences with the Senate. There is no mention in the Report of the COS taking any

[8] See https://www.federalregister.gov/documents/2021/06/25/2021-13554/privacy-act-of-1974-system-of-records
[9] VA Handbook 6300.5, published August 3, 2017, page 8.
[10] See https://www.federalregister.gov/documents/2022/05/20/2022-10844/privacy-act-of-1974-system-of-records
[11] See https://sam.gov/opp/309b11fe7f7246fe8de9d2156a9523e7/view, see also PWS_VIEWS.docx.

substantive action on the matter beyond requesting an in-house investigation. The Report also states that the catalyst for the briefing to the House Committee on Veterans Affairs was "undetermined." See Report, page 11. However, the VA claimed that the COS instructed VA to conduct that briefing.

The COS stated that the allegations she received were around the time she received the OSC order to investigate, and that COS ceased communicating with the whistleblowers so as not to interfere in that investigation. See Report, pages 7, 10. Following up with the whistleblowers to make sure their issues were resolved would not in any way interfere with the VA's own internal investigation. Instead, it seems COS is now making that post hoc argument to evade accountability for failing to act in an appropriate manner.

IV. Report Contradicts Chief of Staff's QFR Answers To Senate

There exists *prima facia* evidence demonstrating privacy breaches despite VA failing to address documentary and testimonial evidence provided to the Senate, OSC, and COS, directly. In the copy of the Report received from the VA, the Report author stated:

- Further analysis remains to be performed regarding recent changes. Moreover, more work is needed to ensure sensitive personal information is not accessible by individuals who do not possess a business need for such information. For example, there is no program of auditing or detection in place to measure the effectiveness of applied changes, or to flag when a user views whistleblower identities and sensitive personal information without authority or fails to protect such information by not setting the appropriate case sensitivity marker.

- 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.

The first statement confirms that "there is no program of auditing or detection in place…to flag when a user views whistleblower identities and sensitive personal information without authority or fails to protect such information by not setting the appropriate case sensitivity marker." This is in conflict with the second statement above, which is misleading. When users view whistleblower identities and sensitive personal information without authority, it is a data breach per the definition below. If not a data breach, it is minimally an incident that must be investigated fully to determine the extent of a data breach, if any. Additionally, if VA has no way of knowing how many times an unauthorized viewer views the data, it is impossible to state that there is no harm caused by VIEWS vulnerabilities.

The Report on page 17 asserts that "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." Though, on page 7, the Report states that, "The whistleblowers believe that the accessibility and sharing of this information has resulted in their mistreatment by managers and co-workers, to include retracted detail opportunities, communicated threats, and vandalism to personal property (all reported separately)." There is "no evidence of harm"

because the VA does not have a platform in place to audit a person that views a VIEWS record, regardless of a "need to know" analysis. The report states "there is no program of auditing or detection in place to measure the effectiveness of applied changes, or to flag when a user views whistleblower identities and sensitive personal information without authority or fails to protect such information by not setting the appropriate case sensitivity marker." It is misleading for VA to state there was no evidence suggesting a data breach of sensitive personal information occurred and/or no harm caused.

The VA's statement above in the Report contradicts both the VA's response to the June 15, 2023 questions from Senator Moran to the COS and the VA's response to the July 11, 2023 Memorandum addressing the SVAC Minority memo:

> **VA states in Response to Senator Moran's question #6:**
>
> **6. In your response to committee questions about sensitive information unsecured in VIEWS, you said that VIEWS, "does not handle medical records, claims, benefits, or financial actions." You also noted that, "the VIEWS system has controls in place to protect personal and sensitive data, with only specific designated team members permitted to access sensitive cases… All employees using VIEWS must complete mandatory training, and system access is logged. Audits also are done to make sure information on the VIEWS system is accessed appropriately" d. When a case is marked sensitive, are unauthorized viewers able to view anything about that case, even if they aren't able to view the attachment or body of the text? For example, are they able to view the title of the email or attachments?** No. A user who is not a member of the specific Case Team will be able to see only the Case ID number and a banner message indicating that they should contact the Case Owner for more information

VA additionally states in their memo to the Senate Committee of Veterans Affairs: "The VIEWS system has controls in place to protect personal and sensitive data, with only specific designated team members permitted to access sensitive cases. Any other user lacking permission who attempts to access a sensitive case cannot see the case information or attachments relating to the sensitive matter."

However, in the copy of the report the OSC received from the VA, VA states:

- Further analysis remains to be performed regarding recent changes. Moreover, more work is needed to ensure sensitive personal information is not accessible by individuals who do not possess a business need for such information. For example, there is no program of auditing or detection in place to measure the effectiveness of applied changes, or to flag when a user views whistleblower identities and sensitive personal information without authority or fails to protect such information by not setting the appropriate case sensitivity marker.

V. VA Waited 11 months to Implement Updates that Significantly Addressed the Issues

The VA's so-called fixes were not timely and failed to fully address the issues, as in the 2019 incident addressed in the Report. It appears VA waited until July (11 months after the issue was reported) to implement updates that significantly addressed the issues with VIEWS. Page 7 of the Report notes that "Some associated fields remained searchable and viewable until very recently… such as the case title and description." This is contrary to an answer the COS provided to the Senate indicating that those fields were not viewable.

This is a lack of veracity, candor and/or evidence of incompetence as to the VIEWS program. VIEWS is a Salesforce contract under OI&T, the investigator interviewed the Salesforce Architect Manager, and VA's reccomendations include additional Salesforce programs. This is a conflict of interest and for these and other reasons, VA should not be investigating its own data breach.

The CFR defines data breach as: *Data breach* means the 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.

But later states: *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). Even after notice of the breach, and requests to remove the whistleblower's pii, confidential communications, sensitive, and personal information to the Veterans Affairs Branch Chief of Privacy Risk Management & Compliance, Veterans Affairs Chief of Staff, Veterans Affairs Office of Inspector General, Government Accountability Office, House Committee of Veterans Affairs, Senate Committee of Veterans Affairs, etc… the VA left whistleblower's personal sensitive information exposed for more than a year (and continuously to this day) causing harm as stated in an email to the Veterans Affairs Chief of Staff on July 13, 2022. The VA's statement that "it should be emphasized that there is no evidence that VIEWS vulnerabilities discussed in this report resulted in a privacy breach or has cause harm to…whistleblowers" lacks veracity, candor, and is evidence of incompetence as to operating the VIEWS system.

Evidence was submitted by whistleblowers proving that a privacy breach occurred and that there was harm to whistleblowers. The VA contradicts itself later in the Report on pages 14 and 19 by stating:

The investigation of this case has been made unusually complex by a wide spectrum of past and current disclosure, litigation, grievance, and activist activities involving and shared by the whistleblowers. In an effort to provide clarity and actionable results, this investigation is focused on the primary allegations regarding sensitive personal information contained in VIEWS CCM and does not attempt to pursue the myriad other concerns that the whistleblowers may have reported to or shared with other oversight entities.

Whistleblowers Allegations

The whistleblowers have made prior disclosures, some of which have resulted in significant public attention. According to the whistleblowers, a VIEWS CCM search for whistleblower names, conducted using a user profile, resulted in access to unsecured cases and correspondence regarding the whistleblowers' previous disclosure activities, as well as other sensitive cases with which the whistleblowers had only incidental association (for example, a complaint received from a Veteran that included the whistleblower as an info addressee). The whistleblowers contend that also visible was sensitive personal information, such as dates of birth and social security numbers of the whistleblowers and persons with associated cases. The whistleblowers believe that the accessibility and sharing of this information has resulted in their mistreatment by managers and co-workers, to include retracted detail opportunities, communicated threats, and vandalism to personal property (all reported separately). The whistleblowers stated that they learned about sensitive information being accessible in VIEWS CCM through various means and reported their concerns to the VA Inspector General and a VA Deputy Chief of Staff (DEPCOSVA), as well as other entities outside of VA. One whistleblower received email responses from the DEPCOSVA saying that they would look into the matter, but the whistleblower stated that no further communication was received from the DEPCOSVA. The DEPCOSVA stated that OIT

VA has evidence of harm but chose not to address it "in an effort to provide clarity and actiionable results." Consequently, it is misleading and lacks veracity to state:

- 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.

VI. Confidential Whistleblower Information Not Secure, Still

On Page 20 of their report, VA admits that current searches performed still return cases and files containing whistleblower identification and sensitive personal information…" They state:

VA employees. Current searches performed using the same key terms still return cases and files containing whistleblower identification and sensitive personal information, but to a significantly lesser degree.

Without a risk assessment and/or an investigation by an outside entity or the OIG, it is impossible to determine the harm caused as well as irreparable future harm as the VA admits the problem is not fixed.

As of August 9, 2023, my personal information, pii, and confidential whistleblower communications are still visible in VEWS. On page 20, VA states:

> In addition to case files containing sensitive personal information, all VIEWS CCM users have access to Veteran names, dates of birth, and personal addresses and phone numbers contained in 3.6 million records in the VIEWS CCM Contacts Database. Cases which relate to a Veteran with a record in this database possess a hyperlink that will take a user to the Veteran's record. This record contains the Veteran's sensitive personal information, as well as links to other VIEWS cases related to that Veteran.

> For those cases that had been incorrectly designated as "Not-Sensitive," any of the approximately 2,010 active VIEWS CCM users can view, download, copy, screenshot, or otherwise share sensitive information – e.g., whistleblower and Veteran social security numbers, dates of birth, home addresses and phone numbers, and medical and financial information – without a need-to-know, and without the authorization or knowledge of business and system owners.
>
> It is difficult to assess the number of cases not marked "Sensitive" that contained whistleblower and Veteran sensitive personal information prior to recent remediations activities due to how VIEWS CCM returns search results. Basic search results are initially returned as a group of five, with the ability to expand results to groups of 50. Active cases and archived cases are returned as separate results. Searching on Case Title versus Case Attachment may produce different results, and variables in case and attachment titling methodologies do not always provide full indication of the contents, requiring each case or file to be individually opened to assess contents. Considering that over 200,000 cases were created over the past three calendar years alone, and the rate at which the presence of sensitive personal information can be found in cases, the "Not Sensitive" cases containing sensitive personal information before remediation actions were implemented is easily estimated to have been in the multi-thousands at the time that the whistleblowers came forward with the allegations.

The statements in the copy of the report the OSC received from the VA, contradict the VA's response to the July 11, 2023 Memorandum of SVAC Minority Staff, where they state:

4. The SVAC Minority staff memorandum concludes, based on the demonstration of the VIEWS system provided by VA, that "thousands" of VIEWS files are not being treated as sensitive files. In fact, the demonstration to the staffers showed no such thing.

According to the staff memorandum, during the VIEWS demonstration on July 7, 2023, "a search for the term 'whistleblower' revealed countless case files containing highly sensitive information—including the names of whistleblowers—not currently designated as 'sensitive' in the system." Staff Mem. pp. 2, 6. It is true that the demonstration showed that the "whistleblower" search showed numerous files that were not marked as sensitive. However, *these documents marked as non-sensitive contained only generic information about whistleblowers and did not contain individual whistleblower information*. For example, these files identified in the search contained memorandum and directives relating to the general procedures for handling whistleblower complaints, drafts of general reports relating to the performance of the Office of Accountability and Whistleblower Protection, comments on whistleblower legislation, and the like. *Nothing in this search showed that files with the names of whistleblowers were not treated as sensitive.*

The staff memorandum's conclusion that thousands of VIEWS files are not being properly treated as sensitive is misguided. The OIT/OSC investigation has been reviewing this very issue about the confidentiality and security of VIEWS. This investigation already has acknowledged in its extension requests that VA has recently implemented actions to protect Veterans' private information and whistleblowers. As Ms. Bradsher has recognized, the investigation is the proper forum to review these VIEWS issues. And she has committed to carefully considering the results of the OIT/OSC review and taking whatever steps are necessary to ensure that the confidentiality of whistleblower and Veteran sensitive information is properly protected.

* * *

The Secretary assigning the investigation to OI&T is a violation of the VA's own Veteran Affairs Information Security Act as it is clear that publishing this information to 2100 people without a need to know is not inadvertent nor legal. P.L. 109-461 requires 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. The VA on page 20 of their report states that "cases containing sensitive personal information before remediation actions were implemented is easily estimated to have been in the **multi thousands** at the time the whistleblowers came forward with the allegations."

VII. Veterans Affairs Information Security Act

Title IX of P.L. 109-461, the Veterans Affairs Information Security Act, requires the Veterans Administration (VA) to implement agency-wide information security procedures to protect the VA's "sensitive personal information" (SPI) and VA information systems. P.L. 109-461 was enacted to respond to the May 2006 breach of the personal data of 26.5 million veterans caused by the theft of a VA employee's hard drive from his home.

Pursuant to P.L. 109-461, the VA's information security program is to provide for the development and maintenance of cost effective security controls to protect VA information, in any medium or format, and VA information systems. The information security program is required to include the following elements: periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of VA information and information systems; policies and procedures based on risk assessments that cost-effectively reduce security risks and ensure information security; implementation of security controls to protect the

confidentiality, integrity, and availability of VA information and information systems; plans for security for networks, facilities, systems, or groups of information systems; annual security awareness training for employees and contractors and users of VA information and information systems; periodic testing of security controls; a process for remedial actions; procedures of detecting, reporting, and responding to security incidents; and plans and procedures to ensure continuity of operations. Additionally, the VA Secretary is directed to comply with FISMA, and other security requirements issued by NIST and OMB. The law also establishes specific information security responsibilities for the VA Secretary, information technology and information security officials, VA information owners, other key officials, users of VA information systems, and the VA Inspector General.

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.

I respectfully request an investigation be performed by either a non-VA entity or the VA's Inspector General to 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. I suggest ceasing the VA annual whistleblower training until VIEWS is fixed and there is accountability for the OSC findings because currently the communications are not confidential (as promised in the annual training) which is not legal and directly places a whistleblower in harm's way.

VIII. Claims VA Did Not Substantiate

It appears VA did not make much of an effort to substantiate the claims that they "were unable to substantiate." Pointing to just 3 FOIA productions that included the relevant information is not legally persuasive.

The Report asserts VA was unable to substantiate whether VA Police use VIEWS as a source of information with "no data connections" between the Disruptive Behavior Reporting System, or DBRS, and VIEWS CCM. Without a log system, SORN, or audit capabilities it is impossible to address this allegation accurately.

8/23/2023

[redacted]