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

The Special Counsel

September 3, 2024

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

Re: OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742

Dear Mr. President:

I am forwarding to you reports transmitted to the Office of Special Counsel (OSC) by the Secretary of Veterans Affairs in response to the Special Counsel's referral of disclosures of wrongdoing at the Department of Veterans Affairs (VA) Headquarters, Washington, D.C. The whistleblowers, a VA employee who chose to remain confidential, and former-Senior Program Manager [redacted] and Program Analyst [redacted], who consented to the release of their names, alleged that VA officials engaged in conduct that constituted a violation of law, rule, or regulation. I have reviewed the disclosure, agency reports, and whistleblower comments, and, in accordance with 5 U.S.C. § 1213, I have determined that the reports contain the information required by statute and the findings appear reasonable.[1] The following is a summary of those findings.

The Whistleblower Allegations

The whistleblowers alleged that VA officials violated federal law and VA policies by improperly storing whistleblowers', veterans', and employees' personally identifiable information (PII) in the agency's Veterans Affairs Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) system. The investigation substantiated the allegation and recommended several corrective actions that have been implemented. During the investigation, the whistleblowers also alleged that records in VIEWS CCM were routinely excluded from VA responses to requests under the Freedom of Information Act (FOIA) and the Privacy Act of 1974 (Privacy Act) and that VA Police improperly used VIEWS CCM when investigating individuals suspected of criminal activity. The VA did not substantiate these allegations. The whistleblowers commented on the reports.

[1] OSC referred the allegations to Secretary of Veterans Affairs Denis McDonough for investigation pursuant to 5 U.S.C. § 1213(c) and (d). The Office of Information Technology investigated the allegations and Secretary McDonough reviewed and signed the agency report.

The Agency Reports

In 2018, the VA replaced its case and correspondence management system—the VA Intranet Quorum (VAIQ) system—and began using VIEWS CCM[2] to conduct administrative and correspondence work. This work includes managing and tracking Congressional, White House, and other outside correspondence, as well as managing and tracking agency documents, and assistance provided to Veterans asking about VA programs, services, and benefits. According to the VA, VIEWS CCM is a National Archives and Records Administration (NARA)-certified system of records managed by the Office of the Executive Secretariat (Executive Secretariat). Roughly 260 cases are created in VIEWS CCM each business day. Through cases, VIEWS CCM collects, processes, and retains information on Veterans, their dependents, and VA employees, including whistleblowers, and contractors. Data entered in VIEWS CCM includes information about the correspondence sent to the VA and its sender. As VIEWS CCM tracks and manages the cases created in the system, *i.e.*, the correspondence, more information may be added to the case.

A. The Investigation Substantiated that Searching in VIEWS CCM Using Certain Terms Returned Numerous Cases Containing PII that Any VIEWS CCM User Could View.

VA Directive 6502, *VA Enterprise Privacy Program,* requires PII to be kept confidential and properly controlled, and VA employees using VA information systems must comply with all privacy policies, procedures, and practices and conduct themselves in accordance with annually signed rules of behavior on the disclosure or use of PII. VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information,* establishes the procedures for managing breaches. The VA uses the terms PII and sensitive personal information, which includes personal health information, interchangeably.

While VIEWS CCM has a strong search capability, it can securely manage PII by restricting access to VIEWS CCM cases. This occurs when a VIEWS CCM user—the case owner—creates and marks a case "Sensitive" and assigns VA employees or a team of employees to process the case. The owners of and users assigned to cases marked "Sensitive" can access the contents of that case, while unassigned users cannot. As of the date of the report, an estimated 2,010 employees used VIEWS CCM.

The investigation discovered that whether cases were correctly marked "Sensitive," and thus appropriately restricted, depended on employee diligence. If the case owner incorrectly marked the case "Not-Sensitive," the case contents could be seen, downloaded, or copied by any active VIEWS CCM user. The investigation also discovered that users assigned to a "Not-

[2] VIEWS CCM runs on the Salesforce Government Cloud Plus (SFGCP) Platform. It is hosted on the U.S. Government Cloud Plus—a Federal Risk and Authorization Management Program (FedRAMP) High approved platform—on Amazon Web Services (AWS) GovCloud and classified as a Minor application under the Major Application SFGCP.

Sensitive" case could add to the case documents or notes containing PII. The investigation revealed the VA could not determine exactly how many cases marked "Not Sensitive" had PII, but estimated the number to be multi-thousands at the time of the whistleblowers' disclosure. The investigation discovered that VIEWS CCM has a Veterans Contacts Database that contains veterans' PII such as DOBs, personal addresses, and phone numbers. The investigation further discovered that when cases in VIEWS CCM related to veterans with records in the Veterans Contacts Database, any VIEWS CCM user could access the database via a hyperlink.

The investigation also revealed that VIEWS CCM tracked changes users made to case information but could not track when users viewed case information or downloaded files. Consequently, the investigator requested case and file access history from the VA's OIT Data Transformation Center (DTC), which maintains the VA's Salesforce platforms and related security and networking systems and previously provided such historical reports. During the investigation, however, DTC stated that it could not produce such reports because a recent transition to a new data tool impacted DTC's ability to produce usable audits. Therefore, while the investigation substantiated that cases incorrectly marked "Not-Sensitive" allowed users to access PII without authorization, the investigation could not determine whether such unauthorized access occurred or its frequency.

Given the above findings, the VA implemented several corrective actions. First, the VA mass converted certain designated case types in VIEWS CCM to "Sensitive." This change applied to all open and closed cases with the designated case types. Additionally, all archived cases from VAIQ were changed to a "Sensitive" status so that only the Office of the Executive Secretariat (Executive Secretariat) can access them. The VA restricted access to the Veteran Contacts Database to only those VIEWS CCM users with a validated business need for the information and reconfigured system business rules for case type and case sensitivity.

The VA changed the default case sensitivity indicator for the following case types: Congressional, White House, and Veteran Case Mail; Investigations and Audits; Investigations and Audits (Non-Government Accountability Office report); and Personnel Matters. Now, when users create a new case for the above case types, the case sensitivity indicator automatically defaults to "Sensitive;" the VA confirmed that this change captures, and thus marks as sensitive, all correspondence received from OSC, the Office of Accountability and Whistleblower Protection, and Offices of Inspector General. Further, all other case types require the user to choose either "Sensitive" or "Not Sensitive" when creating a case and a case cannot be created unless a case sensitivity option is selected. Moreover, the Executive Secretariat now conducts a monthly search in VIEWS CCM for any cases containing PII, but not marked "Sensitive." If such cases are found, they are reported to the Chief of Staff of the Administration or Staff Office from which the case originated, and progressive discipline is imposed on the responsible party. The VA determined that attempting to retrospectively identify users who previously opened VIEWS CCM cases with incorrect case sensitivity would be an ineffective allocation of resources given

the questionable feasibility of the project due to the system changes and the hundreds or thousands of man-hours estimated for such a project. Nevertheless, each time a user accesses VIEWS CCM, a splash page reminds the user that the system and their use thereof are subject to monitoring and review. Also, the VIEWS Office Coordinators conduct quarterly reviews of VIEWS CCM user account rosters looking for accounts that need to be deactivated because the user no longer requires access. Also, the appropriate Chiefs of Staff review and certify the VIEWS CCM user accounts for their offices biannually. Accounts are also suspended after 45 days of inactivity.

In March 2024, the Executive Secretariat also chartered the VIEWS CCM Change Control Board (CCB), which is comprised of officials from the Executive Secretariat, the Veterans Benefits Administration, the Veterans Health Administration (VHA), the Office of Human Resources and Administration/Operations, Security, and Preparedness, the Office of Accountability and Whistleblower Protection, the Office of Congressional and Legislative Affairs, the Office of General Counsel, and OIT. The CCB is responsible for and has the authority to review, approve, and implement functional changes requested to VIEWS CCM, its underlying business processes, and/or governance strategies. The CCB met on March 27, 2024, and the Executive Secretariat has chaired additional meetings since then as needed. At a minimum, the CCB meets to review changes requested for each standard product release.

The Executive Secretariat also hosted live instructor-led sessions for VIEWS CCM users that covered VIEWS CCM procedures and protecting sensitive information. In addition, the VA is developing and updating web-based training courses, to be implemented by the third quarter of fiscal year 2024, which include information about the enhanced security features within VIEWS CCM. The VA is also updating Directive 6508 - *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*, and Handbook 6508.1 - *Procedures for Privacy Threshold Analysis and Privacy Impact Assessment* to reflect current policies, procedures, responsibilities, definitions, and terminologies; the revised documents are expected to be completed in the fourth quarter of fiscal year 2024. (OSC requests that it be provided a copy of these documents upon VA's completion of them.)

Additionally, in 2024, OIT implemented Splunk Enterprise and Salesforce Customer Relationship Management Analytics to detect and report suspicious VIEWS CCM user behavior. The VA has also consulted with the VIEWS CCM Information System Security Officer and other stakeholders to identify suspicious behavior to be audited, including users accessing the system outside of normal business hours and searching or accessing case records when they are not assigned to the case. The VA also installed the Einstein Data Detect application and OIT drafted operating instructions for Salesforce System Administrators to begin scanning VIEWS CCM for Social Security Numbers (SSN) in "Not-Sensitive" cases. Finally, the VA created a strategy to develop standard operating procedures for responding to SSN and suspicious behavior detections. This includes developing business and technical policies that describe the roles,

responsibilities, tasks, reporting methods, and follow up actions expected when these problems are detected. This work is ongoing and will be managed by the CCB.

B. The Investigation Did Not Substantiate that VA Officials Failed to Include VIEWS CCM Searches in FOIA and Privacy Act Requests.

FOIA Officers are required to conduct and document searches reasonably calculated to produce records relevant to a request. Therefore, if a request has a VIEWS CCM nexus, the FOIA Officer searches VIEWS CCM, documents the search, reviews any relevant records, and makes a release determination. During the investigation, the FOIA Office identified recent cases where they searched VIEWS CCM, reviewed material for relevancy and released the material to the requester. The VA Privacy Service was unable to provide any specific cases where VIEWS CCM had been searched in response to a Privacy Act request but stated that Privacy Act requests are received and acted upon by offices in the VA, and no central database can be searched for requests involving VIEWS CCM.

C. The Investigation Did Not Substantiate that VA Police Used VIEWS CCM as a Source of Information When Investigating Individuals Suspected of Criminal Activity.

This allegation stemmed from a belief that the Disruptive Behavior and Reporting System (DBRS) and VIEWS CCM were linked. Subject matter experts confirmed that no data connections exist between DBRS and VIEWS CCM. Also, only seven VA Police offices have an employee who can access VIEWS CCM. But given DTC's inability to audit VIEWS CCM user activity, the investigator could not determine if VA Police viewed VIEWS CCM during its investigations.

The Whistleblower Comments

The whistleblowers criticized the length of time it took the VA to investigate and render its reports. The whistleblowers disputed the report's findings and disagreed with the conclusions regarding the unsubstantiated allegations. The whistleblowers also objected to the VA revising Handbook 6500.2 and its definition of data breach during the investigation and disagreed with the revision. The whistleblowers further disagreed with the VA's decision not to determine and hold accountable the VIEWS CCM users who had incorrectly created prior cases in VIEWS CCM as "Not-Sensitive."

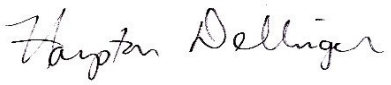
The Special Counsel's Findings

In accordance with 5 U.S.C. § 1213(e) I have determined that the reports contain the information required by statute and the findings appear reasonable. I thank the whistleblowers for bringing these important allegations to OSC's attention. I expect the VA to continue to monitor and audit the VIEWS CCM system in relation to the PII contained therein pursuant to

the implemented corrective actions. OSC also expects to receive the updated documents noted above which VA has committed to have completed and adopted this calendar year. I urge VA's OIG to closely monitor the agency's adherence to VIEWS-related laws, rules and commitments. And, finally, I believe it is imperative that VA leadership cooperate with Congressional requests for information related to VIEWS.

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

Respectfully,



Hampton Dellinger
Special Counsel

Enclosures