THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

November 6, 2023

Ms. Catherine McMullen
Chief, Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, NW, Suite 300
Washington, DC 20036

Re: Office Special Counsel File Nos. DI-22-000680, DI-22-000682 and DI-22-000742

Dear Ms. McMullen:

Enclosed is the supplemental report as requested in your September 13, 2023, email to the Department of Veterans Affairs (VA). The supplemental report provides additional information related to VA's July 21, 2023, report submitted to the Office of Special Counsel on the investigation of the protection of sensitive personal information contained in the VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) system.

Thank you for the opportunity to respond.

Sincerely,

Denis McDonough

Enclosure

Department of Veterans Affairs (VA)
Supplemental Report for the Office of Special Counsel (OSC)
Office of the Executive Secretariat

Washington, DC

OSC File Numbers DI-22-000680, DI-22-000682 and DI-22-000742

July 2023

The VA Office of the Secretary received an email from OSC on September 13, 2023, regarding VA's investigation of whistleblower allegations related to the protection of sensitive personal information contained in the VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) system.
After reviewing the agency report in the above companion referrals, OSC is requesting a supplemental report addressing four questions. OSC's questions and VA's responses are set out below.

OSC Question #1
The agency report used the definition of breach included in the VA Handbook 6500.2 (VA Handbook 6500.2), Management of Breaches Involving Sensitive Personal Information, published June 30, 2023 to make its findings on allegations 1 and 2. In 2023, "breach" is defined 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." However, the 2019 version of VA Handbook 6500.2 was the provision applicable in the years prior to and at the time of OSC's referral on August 2, 2022, and during the pendency of the VA's investigation pursuant to 5 U.S.C. § 1213(c). The 2019 version of VA Handbook 6055.2 defined "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."

Please explain why the agency report relied on the definition of breach in the 2023 version of VA Handbook 6500.2 in reaching its conclusions instead of the 2019 definition of breach applicable at the time of the allegations. Also, explain whether the application of the 2019 definition of the term breach changed any of the report's findings or conclusions related to allegations 1 or 2.

VA Response
VA believes that it is appropriate to rely on the current version of the policy because it contains the most up-to-date and accurate statement of the Department's position. As with most organizations, VA periodically reviews and revises its policies to ensure that they reflect the best and most efficacious thinking on a matter. For this reason, VA believes it would have been misleading to apply an obsolete, inferior policy in its

report. In addition, the statement regarding "privacy breach" in the report's conclusion does not reference the VA policy; rather, the statement correctly reflects how this term is used in common parlance. In both the common plain meaning of "privacy breach" and the current VA Handbook 6500.2 definition, there needs to be an actual instance of unauthorized access for there to be a "breach" and it is not sufficient that there is simply a "potential" for unauthorized access. In this regard, the superseded Handbook's definition is problematic since there is always a "potential" for unauthorized access in even the best systems. 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." See D*oyon v. United States*, 58 F.4th 1235, 1245 (Fed. Cir. 2023) (quoting *Bradley v. Sch. Bd. Of Richmond*, 416 U.S. 696, 711 (1974)). In this instance, there is none of the retroactive effect that would impair rights or impose new duties and thereby preclude applying the current policy to past conduct.

For these reasons, we disagree with the premise of your question about whether the application of the 2019 policy would change any of the VA report's findings or conclusions. Moreover, as noted above, the statement about "privacy breach" in the conclusion of the report did not reference the technical definition of "privacy breach" in the VA Handbook but appears to rely on its plain meaning in common parlance; thus, the Handbook definition is inapplicable. Furthermore, even under the rescinded 2019 Handbook definition, there is no breach when the probability that the information was or could be compromised is low.

OSC Question #2
The report found that based on the number of cases that users incorrectly opened in VIEWS CCM as Not Sensitive—estimated at multi-thousands—Agency policy and training alone have not effectively ensured that VIEWS CCM users managed sensitive personal information and that there has been no effort to hold these violators accountable. Is the agency considering holding any of the VIEWS CCM users accountable for the cases that were incorrectly opened during the relevant time period, particularly users who opened multiple cases incorrectly? If not, why not? Also, is the agency considering whether to implement a mechanism to provide accountability in the future.

VA Response
VA has focused its efforts on improving the VIEWS CCM system to ensure that sensitive personal information is protected and not improperly available on the system. These steps have included moving all Veteran and Congressional case mail, White House case mail, Investigations and Audits and Other case record types to the "Sensitive" designation. This change applied to all open and closed cases from these four case types, which comprise a large portion of the total cases in VIEWS. In addition, all archived cases from the prior case and correspondence management system, VAIQ, have been changed to a "Sensitive" status so that only the Office of the Executive Secretary can access them. Also, the VIEWS CCM system has been changed so that new cases in these four major categories – Veteran and Congressional case mail,

White House case mail, Investigations and Audits and Other – can only be created as "Sensitive." As noted in the report, these measures "have dramatically reduced improper access to sensitive information."

By contrast, 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.

However, VA is focused on ensuring accountability moving forward. In order to check that new cases being added to VIEWS are being created with personal information protected, VA is in the process of developing a monthly audit program. Under this program, each month the Executive Secretary's office will search VIEWS using a list of 18 keywords. Any cases that appear to have personally identifiable information or protected health information and are not marked "Sensitive" will be noted and reported to the chief of staff of the administrative office from which the case originated. Under this program, a progressive discipline approach would be applied to individuals incorrectly opening cases without the proper case sensitivity. VA anticipates having this audit program in place by the end of quarter (Q)1 in fiscal year (FY) 2024.

OSC Question #3
The report identified agency employees by position title but did not attach a key that identifies employees by both name and position. Please provide OSC an unredacted version of this key as requested in OSC's Appendix A included with the referral for investigation on August 2, 2022.

VA Response
VA has no objection to sharing with OSC a key that identifies employees by name and position. However, shortly after VA provided OSC with its report in this matter, details about the VA report (including actual quotations) appeared in various media outlets. In fact, one of the whistleblowers publicly admitted that he had leaked the VA's report. For this reason, VA has concerns if OSC's intentions are to share with the whistleblowers any documents provided by VA containing the key; if that is the case, then VA would propose to make the key available to OSC for review at VA's offices.

OSC Question #4
Please provide the agency's timeline for completing the report's recommended corrective actions and identify any of the recommended corrective actions that have been fully implemented.

VA Response
Please see the information provided below.

VA Office of the Executive Secretariat

Recommendation 1: Continue to work to ensure that sensitive personal and whistleblower information is not accessible by individuals who do not possess a business need for such information, including taking additional steps to:

a. Restrict visibility of Veteran sensitive personal information contained in the contacts database to only those VIEWS CCM users with a validated business need for the information.

   Target Completion Date: Completed on 8/11/2023.

b. Restrict visibility of sensitive personal information contained in VIEWS CCM cases to only those VIEWS CCM users with a validated business need for the information.

   Target Completion Date: Completed on 7/20/2023.

c. Restrict visibility of whistleblower identification and activities contained in VIEWS CCM cases to only those VIEWS CCM users with a validated business need for the information.

   Target Completion Date: Completed on 8/3/2023.

Recommendation 2: Charter a cross-functional team or working group with authority and accountability for assessing the privacy and security of VIEWS CCM, remediating discovered or reported issues, and managing and reporting on recommend actions contained in this report. All major VIEWS CCM stakeholder organizations should be represented on the team, to include user, support and advisory entities such as the Office of Information Technology (OIT), Office of General Counsel (OGC), VA Privacy Service, VA FOIA Service, VA Enterprise Records Service, the Veterans Benefits Administration, and the Veterans Health Administration.

Target Completion Date: Q1, FY 2024.

Recommendation 3: Develop and implement an awareness campaign specifically focused on user management of sensitive information in VIEWS CCM. Consider hosting live instructor-led sessions to demonstrate procedures and address questions, implementing user awareness certifications to document user understanding and enhance accountability, and designating or developing recurring user training to periodically remind users of procedures and responsibilities for protecting sensitive information in VIEWS CCM.

Target Completion Date: Q1, FY 2024.

Recommendation 4: In conjunction with the Office of Information Technology (OIT), continue to pursue the acquisition and deployment of a data tool, such as Einstein Data Detect and FairWarning, to automatically detect and report suspicious VIEWS CCM user behavior, and to provide forensic auditing of user activities that do not modify case information or files, such as browsing, searching, viewing, and downloading records and files.

Target Completion Date: Completed on 8/11/2023.

Recommendation 5: Develop and implement an auditing program of VIEWS CCM cases and user activities that supports effective policy enforcement and enhances user accountability.

Target Completion Date: Q1, FY 2024.

Recommendation 6: Consider changing the default sensitivity indicator for all new cases to "Sensitive" to force a sensitivity determination during case initiation.

Target Completion Date: Q1, FY 2024.

Recommendation 7: Consider adding a highly visible banner to all cases marked "Not Sensitive." In the banner, include a warning that the selected case is not authorized for sensitive personal information, and that the user should mark the case "Sensitive" if intending to add sensitive personal information to the case.

Target Completion Date: Completed on 9/28/2023.

VA Privacy Service

Recommendation 1: Update VA 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 accurately reflect current policies, procedures, responsibilities, definitions, and terminologies.

Target Completion Date: Q1, FY 2024.

Recommendation 2: Develop and publish written procedures for the confidential reporting of privacy incidents.

Target Completion Date: Completed on 6/30/2023.

Recommendation 3: Consider including IT system Business Owners as signatories on all Privacy Threshold Analysis (PTA) and Privacy Impact Assessments (PIA) to enhance accountability and ensure all relevant business practices and user procedures are fully represented in the PTA and PIA.

Target Completion Date: IT System Owners currently sign the PTA/PIAs, in accordance with VA Directive 6508.

Recommendation 4: Consider implementing a customer-facing online incident intake tool as a companion to the Privacy and Security Event Tracking System (PSETS) to ensure that all incident reports are received, documented, and appropriately investigated, and that the person reporting the incident receives timely feedback.

Target Completion Date: The VA Data Breach Review Service (DBRS) is responsible for privacy breach management within VA and communicates that privacy incidents require detailed reporting of data elements to meet the Cybersecurity and Infrastructure Security Agency, Privacy Act of 1974 and Health Insurance Portability and Accountability Act of 1996 requirements, of which Privacy Officers and Information System Security Officers are familiar. A customer-facing tool would make it cumbersome for the reporting individual, due to their unfamiliarity with the incident reporting requirements, and delay the processing and management of the privacy incident. In addition, there are currently several avenues for reporting privacy incidents available to customers.

VA requests closure of this recommendation.

VA Office of Information and Technology

Recommendation 1: Conduct a Security Controls Assessment on VIEWS CCM and report results and recommendations to relevant stakeholders for appropriate action.

Target Completion Date: Completed on 10/11/2023.

Recommendation 2: In conjunction with the Executive Secretariat/VIEWS CCM Business Owner, continue to pursue the acquisition and deployment of a data tool, such as Einstein Data Detect or FairWarning, to automatically detect and report suspicious VIEWS CCM user behavior, and to provide forensic auditing of user activities that do not modify case information or files, such as browsing, searching, viewing, and downloading records and files.

Target Completion Date: Q3, FY 2024.

Recommendation 3: Continue to refine IT system security assessment and approval procedures to improve the effectiveness of system security features and controls, particularly those with impact on the protection of sensitive personal information.

Target Completion Date: Q1, FY 2025.

Department of Veterans Affairs
November 2023