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

The Special Counsel

August 2, 2022

The Honorable Denis McDonough
Secretary
Department of Veterans Affairs
810 Vermont Avenue, N.W.
Washington, D.C. 20420

Re: OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742
Referral for Investigation − 5 U.S.C. § 1213(c)

Dear Secretary McDonough:

I am referring to you for investigation a whistleblower disclosure that employees at the U.S. Department of Veterans Affairs (VA), Washington, D.C., engaged in conduct that may constitute a violation of law, rule, or regulation. A report of your investigation of these allegations and any related matters is due to the Office of Special Counsel (OSC) by October 3, 2022.

The whistleblowers, one VA employee who chose to remain anonymous, and former-[redacted] and [redacted], who consented to the release of their names, disclosed that VA officials are violating federal law and VA policies by improperly storing the personally identifiable information (PII) of whistleblowers, employees, and veterans in the Veterans Affairs Integrated Enterprise Workflow Solution (VIEWS) system of records.[1] The whistleblowers allege that the VIEWS system does not comply with the Privacy Act and VA policies because sensitive information is not marked as sensitive and is therefore accessible to all VA employees that have access to VIEWS—not just those employees with a need to know the information. The allegations to be investigated include:

- VA employees have failed to protect the confidentiality of whistleblowers' identities, their submissions, and PII in VIEWS, in violation of federal law and agency directive and handbook provisions;

[1] *See* Privacy Act of 1974 (codified at 5 U.S.C. § 552a); *see also* VA Directive 6502 *VA Enterprise Privacy Program* (VA Directive 6502), and VA Handbook 6500 *Risk Management Framework for VA Information Systems VA Information Security Program* (VA Handbook 6500). Specifically, VA Directive 6502 applies the VA Privacy Program to all veteran and employee PII that the VA maintains, regardless of the medium in which the data is kept and directs the VA to protect the privacy of such data in compliance with the requirements of all federal statutes and regulations, Executive Orders, and government and VA-wide policies, procedures, and guidance. Similarly, VA Handbook 6500 states that the Chief Privacy Officer shall develop system-level privacy policies and procedures and ensure compliance with the same, and the Privacy Officer shall monitor a system and its operational environment to develop and update privacy plans with other relevant VA offices.

- VA employees have failed to protect the confidentiality of veterans' PII in VIEWS, in violation of federal law and agency directive and handbook provisions; and
- Any additional, related allegations of wrongdoing discovered during the investigation of the foregoing allegations.

The VA corresponds with veterans, their families, the White House, Congress, state and local officials, government agencies, and stakeholders. To track and respond to this correspondence, the VA implemented VIEWS in approximately 2018 to replace legacy systems. When the VA receives correspondence, employees upload it and any related documents—e.g., enclosures, attachments, e-mails, draft replies—to VIEWS by creating a "case;" each "case" in VIEWS relates to correspondence the VA received. Creating a case for the correspondence allows employees to assign and track all work needed to reply to the correspondence and VIEWS allows the employee to mark a case as sensitive or non-sensitive. *See VIEWS Quick Reference Guide Case Sensitivity*. Marking a case as sensitive limits which employees can access and review the information. *See id*. Cases marked as non-sensitive allow any general VIEWS user to see the case information. Cases containing PII or personal health information and all congressional correspondence are to be marked sensitive. *See id.*; *see also VIEWS Case and Correspondence Management New User Guide* (2020).

The whistleblowers alleged that VA employees have failed to mark as sensitive thousands of cases containing congressional correspondence, whistleblower identities and/or submissions, and whistleblowers' and veterans' PII. The whistleblowers stated that conducting a general search in VIEWS of words or terms such as "whistleblower," "disclosure," "Congressional," "SSN," "DB214," "OAWP," "OSC," and "OIG" returned thousands of case results marked non-sensitive, and Privacy Act protected information that should have had limited access. For example, [redacted] searched VIEWS using the term "SSN" and found thousands of non-sensitive cases, files, and other VIEWS entries that contained employees' and veterans' social security numbers, which could be seen when the user accessed the case or when the user hovered the cursor over a VIEWS entry called "description field." The whistleblowers have additional documentation regarding sample search results.

Pursuant to my authority under 5 U.S.C. § 1213(c), I have concluded that there is a substantial likelihood that the information provided to OSC discloses a violation of law, rule, or regulation. Please note that specific allegations and references to specific violations of law, rule or regulation are not intended to be exclusive. If, in the course of your investigation, you discover additional violations, please include your findings on these additional matters in the report to OSC. As previously noted, your agency must conduct an investigation of these matters and produce a report, which must be reviewed and signed by you. Per statutory requirements, I will review the report for sufficiency and reasonableness before sending copies of the agency report along with the whistleblower's comments and any comments or recommendations I may have, to the President and congressional oversight committees and making these documents publicly available.

Additional important requirements and guidance on the agency report are included in the attached Appendix, which can be accessed at https://osc.gov/Services/Pages/DU-Resources.aspx. If your investigators have questions regarding the statutory process or the report required under 5 U.S.C. § 1213, please contact Catherine A. McMullen, Chief, Disclosure Unit, at (202) 804-7088 or cmcmullen@osc.gov for assistance. I am also available for any questions you may have.

Sincerely,

Henry J. Kerner
Special Counsel

Enclosure
cc: The Honorable Michael J. Missal, VA Inspector General

APPENDIX
AGENCY REPORTS UNDER 5 U.S.C. § 1213

GUIDANCE ON 1213 REPORT

- OSC requires that your investigators interview the whistleblower at the beginning of the agency investigation when the whistleblower consents to the disclosure of his or her name.
- Should the agency head delegate the authority to review and sign the report, the delegation must be specifically stated and include the authority to take the actions necessary under 5 U.S.C. § 1213(d)(5).
- OSC will consider extension requests in 60-day increments when an agency evidences that it is conducting a good faith investigation that will require more time to complete.
- Identify agency employees by position title in the report and attach a key identifying the employees by both name and position. The key identifying employees will be used by OSC in its review and evaluation of the report. OSC will place the report without the employee identification key in its public file.
- Do not include in the report personally identifiable information, such as social security numbers, home addresses and telephone numbers, personal e-mails, dates and places of birth, and personal financial information.
- Include information about actual or projected financial savings as a result of the investigation as well as any policy changes related to the financial savings.
- Reports previously provided to OSC may be reviewed through OSC's public file, which is available here: https://osc.gov/Pages/Resources-PublicFiles.aspx. Please refer to our file number in any correspondence on this matter.

RETALIATION AGAINST WHISTLEBLOWERS

In some cases, whistleblowers who have made disclosures to OSC that are referred for investigation pursuant to 5 U.S.C. § 1213 also allege retaliation for whistleblowing once the agency is on notice of their allegations. The Special Counsel strongly recommends the agency take all appropriate measures to protect individuals from retaliation and other prohibited personnel practices.

EXCEPTIONS TO PUBLIC FILE REQUIREMENT

OSC will place a copy of the agency report in its public file unless it is classified or prohibited from release by law or by Executive Order requiring that information be kept secret in the interest of national defense or the conduct of foreign affairs. 5 U.S.C. § 1219(a).

EVIDENCE OF CRIMINAL CONDUCT

If the agency discovers evidence of a criminal violation during the course of its investigation and refers the evidence to the Attorney General, the agency must notify the Office of Personnel Management and the Office of Management and Budget. 5 U.S.C. § 1213(f). In such cases, the agency must still submit its report to OSC, but OSC must not share the report lower or make it publicly available. See 5 U.S.C. §§ 1213(f), 1219(a)(1)