THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

August 8, 2023

The Honorable Henry Kerner
Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW, Suite 300
Washington, DC 20036

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

Dear Mr. Kerner:

I am responding to your August 2, 2022, letter regarding whistleblower allegations concerning the Veterans Affairs Integrated Enterprise Workflow Solutions (VIEWS) system and related matters.

I directed that the Office of Information Technology (OIT) investigate these allegations. Enclosed is the OIT report which addresses each of the allegations raised by the whistleblowers. The OIT report also includes a number of recommendations for the Executive Secretariat, VA Privacy Service, and OIT. VA concurs in these recommendations, and the report will be sent to the respective offices with a request for an action plan. You will note that one recommendation is to charter a cross-functional team or working group to oversee implementation of improvements to the system. I have now directed that the Office of Accountability and Whistleblower Protection – our office charged with whistleblower protection – join that team or working group.

VA takes allegations of this nature seriously and appreciates the opportunity to review this important matter and the whistleblowers' diligence in raising their concerns. Thank you for the opportunity to respond.

Sincerely,

Denis McDonough

Enclosure

DEPARTMENT OF VETERANS AFFAIRS

Washington, DC

Report to the
Office of Special Counsel
OSC File Nos. DI-22-000680, DI-22-000682, and DI-22-000742

Office of the Executive Secretariat
Washington, DC

Report Date: July 21, 2023

Executive Summary

The Secretary of the Department of Veterans Affairs directed that the Office of Information Technology investigate whistleblower disclosures made to the Office of Special Counsel (OSC) concerning sensitive personal information contained in the Veterans Affairs Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) system managed by the VA Office of the Executive Secretariat, located in Washington, DC. Three whistleblowers, two of whom had previously raised whistleblowing complaints on other subjects and were VA employees at the time of this disclosure, alleged that VA officials are violating federal law and VA policies by improperly storing the sensitive personal information of thousands of whistleblowers, Veterans, and employees in VIEWS CCM, and allowing unrestricted access to nearly 2,010 system users. During the course of the investigation, the whistleblowers additionally alleged that VIEWS CCM is improperly used by VA Police as a source of information on people being investigated for suspected criminal activity, and that records contained in VIEWS CCM are routinely excluded from agency responses to FOIA and Privacy Act requests. We conducted a virtual investigation from October 3, 2022, to July 21, 2023.

Specific Allegations of the Whistleblowers

1. *VA officials 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.*

2. *VA officials have failed to protect the confidentiality of veterans' PII in VIEWS, in violation of federal law and agency directive and handbook provisions.*

3. *VA officials have failed to include VIEWS in FOIA and Privacy Act requests, in violation of federal law and agency directive and handbook provisions.*

4. *VA Police use VIEWS as a source information on people who are being investigated for suspected criminal activity, in violation of federal law and agency directive and handbook provisions.*

We **substantiated** allegations when the facts and findings supported that the alleged events or actions took place and **did not substantiate** allegations when the facts and findings showed the allegations were unfounded. We were **unable to substantiate** allegations when the available evidence was insufficient to support conclusions with reasonable certainty about whether the alleged event or action took place.

After a careful review of the evidence, we make the following conclusions and recommendations.

Key Findings and Conclusions for Allegations 1 and 2

- We **substantiate** that, although they have undertaken substantial efforts and made considerable strides in improving the protection of sensitive information in VIEWS, VA officials still need to take additional measures to protect the confidentiality of whistleblower identities, their submissions, and PII in VIEWS CCM, as well as the confidentiality of veterans' PII in VIEWS, to ensure against violations of the Privacy Act, the Whistleblower Protection Act and VA Directive 6502.

- The system business owner was aware that there likely were a significant number of cases containing sensitive personal and whistleblower information that were not appropriately marked and not protected from unauthorized access by system users. The business owner noted that given the large volume of cases and thousands of VIEWS users, it was inevitable that some users had not marked cases appropriately, contrary to their training and VA policy.

- Following the issues about sensitive information in VIEWS CCM being first raised by whistleblowers, the system business owner took steps to improve and remediate privacy issues. However, some users did not appropriately mark cases that contained personal, PII or whistleblower information as sensitive. In those cases where the case users have not appropriately marked a case as sensitive, VIEWS CCM users are allowed access to this sensitive personal or whistleblower information without respect to their functional role and real or potential need to access such information.

- More recently, changes applied to VIEWS CCM in July 2023 significantly reduced the accessibility of whistleblower identities and sensitive personal information contained in archived and active cases, by mass converting designated case types to "sensitive" and reconfiguring system business rules for case type and case sensitivity.

- System users can still search for and view whistleblower identities and sensitive personal information, although to a much less degree, found in cases with blank or "Pending Review" case sensitivity indicators, in disassociated case files, and in the Veterans contacts database. This ability is not restricted to a user's functional role or need to access such information.

- 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 assessment processes employed to authorize the operation of VIEWS CCM, although in compliance with VA IT policy, failed to meet the objective of identifying and mitigating privacy and security risks associated with the use of sensitive personal information. The practice of referring security assessments for minor applications to parent applications, although expedient, may have led to the failure of the identification and mitigation of privacy vulnerabilities unique to VIEWS CCM.

- The VA Privacy Service failed to appropriately respond to and remediate a privacy incident reported by a whistleblower. The Service's response, as monitored throughout the period of this investigation, was not timely and provided incorrect information to the whistleblower regarding the accessibility of files in VIEWS CCM containing their identity, whistleblower activities, and sensitive personal information. Additionally, the response was inconsistent with that of a previous near identical report made by another whistleblower where an appropriate process was followed.

Recommendations to the VA Office of the Executive Secretariat

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.

    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.

    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.

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.

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.

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.

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

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

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.

Recommendations to the VA Privacy Service

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.

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

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.

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.

Recommendations to VA Office of Information and Technology

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

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.

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.

Key Findings and Conclusions for Allegation 3

- We were **unable to substantiate** that VA officials have failed to include VIEWS in FOIA and Privacy Act requests, in violation of federal law and agency directive and handbook provisions.

- When asked, the VA FOIA Office was able to quickly identify at least three recent cases where VIEWS CCM was searched, and material was reviewed for relevancy and ultimately released to the requester. FOIA Officers are required to conduct and document searches reasonably calculated to produce records relevant to a request. Because of this standard, if a request has a VIEWS CCM nexus, the FOIA Officer will search VIEWS CCM, document that search, review any relevant records, and make a release determination.

- When asked, the VA Privacy Service was unable to provide any specific cases in which VIEWS CCM had been searched in response to a Privacy Act request but stated that Privacy Act requests were received and independently acted upon by offices across VA, and that there was no central database that could be searched for requests involving VIEWS CCM.

Recommendations

There are no recommendations specific to this allegation.

Key Findings and Conclusions for Allegation 4

- We were **unable to substantiate** that VA Police use VIEWS as a source information for people who are being investigated for suspected criminal activity, in violation of federal law and agency directive and handbook provisions.

- During interviews of witnesses, we found that this allegation stemmed from a belief that the Disruptive Behavior and Reporting System (DBRS), implemented as a part

the Veterans Health Administration (VHA) Workplace Violence Prevention Program (WVPP), was linked to VIEWS CCM making VIEWS CCM information viewable by VA Police.

- Subject matter experts (SMEs) for VIEWS CCM confirmed there were no data connections between DBRS and VIEWS CCM.
- VA Police do not access information in VIEWS CCM through a DBRS interface, as such an interface does not exist.
- Only seven VA Police offices have VIEWS CCM access; each of these offices has a single employee as a VIEWS CCM user.
- Without the ability to conduct comprehensive audits of VIEWS CCM user activity, it is not possible to determine if VA Police view and utilize VIEWS CCM as a source of investigative information.
- It is undetermined if such use would violate any laws, rules, or policies.

Recommendations

There are no recommendations specific to this allegation.

Table of Contents

I. Introduction

The Secretary of the Department of Veterans Affairs directed that the Office of Information Technology investigate whistleblower disclosures made to the Office of Special Counsel (OSC) concerning sensitive personal information contained in the Veterans Affairs Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) system managed by the VA Office of the Executive Secretariat, located in Washington, DC. Three whistleblowers, two of whom had previously raised whistleblowing complaints on other subjects and were VA employees at the time of this disclosure, alleged that VA officials are violating federal law and VA policies by improperly storing the sensitive personal information of thousands of whistleblowers, Veterans, and employees in VIEWS CCM, and allowing unrestricted access to nearly 2,010 system users. During the course of the investigation, the whistleblowers additionally alleged that VIEWS CCM is improperly used by VA Police as a source of information on people being investigated for suspected criminal activity, and that records contained in VIEWS CCM are routinely excluded from agency responses to FOIA and Privacy Act requests. We conducted a virtual investigation from October 3, 2022, to July 21, 2023.

II. Facility Profile

The Executive Secretariat is VA's central coordinating point for all staff actions addressed to, and emanating from, the Secretary of Veterans Affairs (SECVA), the Deputy Secretary of Veterans Affairs (DEPSECVA), and the Chief of Staff of Veterans Affairs (COSVA). Activities and responsibilities include acting as the principal staff action control point for the Department on internal and external items, directing and assigning tasks on behalf of SECVA, coordinating with other Federal agencies and departments on joint letters and memoranda, preparing responses to Members of Congress, and serving as the Department's point of contact and response coordinator for U.S. Office of Special Counsel's disclosure cases. The Executive Secretariat is physically located in the VA headquarters in Washington, DC.

III. Specific Allegations of the Whistleblowers

1. *VA officials 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.*

2. *VA officials have failed to protect the confidentiality of veterans' PII in VIEWS, in violation of federal law and agency directive and handbook provisions.*

3. *VA officials have failed to include VIEWS in FOIA and Privacy Act requests, in violation of federal law and agency directive and handbook provisions.*

4. *VA Police use VIEWS as a source information on people who are being investigated for suspected criminal activity, in violation of federal law and agency directive and handbook provisions.*

IV. Conduct of Investigation

This investigation was conducted by the VA Office of Information Technology (OIT) - Compliance, Risk and Remediation Service.

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.

We interviewed the whistleblowers on November 4, 2022, November 8, 2022, and on April 19, 2023. We also interviewed or consulted with the following staff:

- IT Program Manager for Sustainment (VIEWS CCM)
- VA Privacy Officer
- VA Privacy Program Manager
- VA FOIA Officer
- VA Records Officer
- Director, OIT Security Assessment and Validation
- Director, OIT Enterprise Risk Management
- Director, OIT Operational Planning and Remediation
- Supervisory IT Specialist, OIT Operational Planning and Remediation
- President, Whistleblowers of America
- Senior Salesforce Technical Architect (Contractor), OIT Data Transformation Center
- Technical Architect (Contractor), OIT Data Transformation Center
- Program Analyst, Office of the Executive Secretariat
- VA Executive Secretary (VIEWS CCM Business Owner)
- Deputy General Counsel, General Law Group, VA Office of General Counsel
- Deputy Chief Counsel, Information and Administrative Law Group, VA Office of General Counsel
- VIEWS CCM Information System Owner (ISO)
- VIEWS CCM Information System Security Officer (ISSO)

V. Background

Due to the similarities and shared foundation of the allegations, a single background section is provided to address all allegations.

VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM)

In 2018, VA replaced the VA Intranet Quorum (VAIQ) system with the VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) system. VIEWS CCM is managed by the Office of the Executive Secretariat and used by all VA staff and program offices to conduct administrative and correspondence-related work. VIEWS CCM is also used to coordinate documents and materials related to partnerships with other Federal organizations, state, local, tribal, and non-governmental organizations and individuals, as well as international governments and private sector organizations. VIEWS CCM is also used to manage Congressional correspondence, internal documents such as reports, memoranda, and handbooks, responses to White House case mail, and assistance to Veterans making inquiries about VA programs, services, and benefits. VIEWS CCM is a National Archives and Records Administration (NARA)-certified system of records.

The Executive Secretary is the VIEWS CCM Business Owner, the senior official or executive within an organization with specific mission or line-of-business responsibilities, and with a security or privacy interest in the organizational system supporting those missions or lines-of-business. A senior IT Specialist from the Office of Information and Technology (OIT) is the Information System Owner, the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The system also has a designated Privacy Officer and an Information System Security Officer (ISSO). The Privacy Officer is responsible for taking proactive measures to help ensure that PII collected by VA is limited to that which is legally authorized and necessary and is maintained in a manner that precludes unwarranted intrusions upon individual privacy, thereby minimizing privacy events. The ISSO is responsible for maintaining the appropriate operational security posture for the information system.

VIEWS CCM stores information on system users and other persons who have initiated a case or are involved in the subsequent processing of a case. As of the date of this report, there were approximately 2,010 system users.

VIEWS CCM collects, processes, or retains information on Veterans and/or dependents, as well as VA employees and contractors. Data entered into this system is directly related to the correspondence received, including information on the person who sent the request and information in the correspondence. As the correspondence is being tracked and managed, additional information may be added to the system.

The system shares information with Identity and Access Management (IAM) and the Master Person Index (MPI), also called the Master Veterans Index (MVI). MPI is the

VA's authoritative source for personal identity data, providing a universal, unique identification record for Veterans. The MPI integration in VIEWS CCM also serves as a searchable database of verified Veteran contact information. VIEWS CCM uses the MPI to verify a Veteran's identity, attach the Veteran to the case and view existing cases associated with the Veteran. MPI information includes name, email, last four digits of social security number (SSN), birth date and eligibility status. Additional Sensitive Personal Information may include Military Service History, Branch of Service, Place of Birth, Education History, Employment History and Gender.

VIEWS CCM also integrates with KnowWho, a Salesforce App Exchange product that provides a directory of contact and biographical data on all Members of Congress (MOC), Capitol Hill staffers, committees, and caucuses. KnowWho integration with VIEWS CCM allows case owners to search for and attach MOC and their staffers directly to a case as an Associated Contact.

VIEWS CCM runs in the Salesforce Government Cloud Plus (SFGCP), which has been FedRAMP-certified for Platform as a Service (PaaS) and Software as a Service (SaaS) since 2014.

VIEWS CCM was developed and built using the Salesforce Government Cloud Plus Platform, which is Federal Risk and Authorization Management Program (FedRAMP) High approved. It is hosted on the U.S. Government Cloud Plus (FedRAMP High), built on Amazon Web Services (AWS) GovCloud (U.S.). VIEWS is classified as a Minor application under the Major Application SFGCP.

VIEWS CCM has an approval date of June 5, 2023, thru June 5, 2024. The Federal Information Processing Standards (FIPS) 199 classification is Moderate.

Types of Sensitive Personal Information

Sensitive personal information, which comes in many forms, should always be protected. Its protection is covered under laws including the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). VA's Privacy Program also requires appropriate administrative, physical, and technical safeguards to protect personal information and limit the uses and disclosures of such information without an individual's authorization.

VA considers sensitive personal information and PII interchangeable. It uses both terms to refer to any information about an individual that is maintained by VA and can be linked to that individual—for example, medical records maintained by VA that can be linked to an individual through the individual's name, social security number, or date and place of birth. VA considers PHI a subcategory of PII. PHI is health and demographic data transmitted by, or maintained in, electronic or any other form or medium that can be used to identify an individual.

Whistleblower Identity Protection

The Whistleblower Protection Act and the Inspector General Act of 1978 require the confidentiality of whistleblowers. Under the Whistleblower Protection Act (5 U.S.C.§1213(h)), the Office of Special Counsel may not disclose the identity of any individual who makes a protected disclosure without the individual's consent, unless it is "necessary because of an imminent danger to public health of safety or imminent violation of any criminal law." The Inspector General Act (Section 7) requires Inspectors General, and their staff maintain whistleblower confidentiality "unless otherwise unavoidable" or unless the whistleblower provides consent to have their identity shared. In addition, under the Privacy Act of 1974 (5 U.S.C.§552a) it is illegal for the government to publicly disclose personal information about an individual without their consent.

Unauthorized disclosure of this information can be disruptive and damaging to VA's ability to achieve its mission, place the safety and well-being of the whistleblower at risk, and violate federal laws protecting whistleblower identities.

Handling of Sensitive Personal Information

VA Directive 6502, *VA Enterprise Privacy Program*, requires that PII be kept confidential and properly controlled. All VA information system users must comply with all related policies, procedures, and practices. All users of VA information must also conduct themselves in accordance with the annually signed rules of behavior concerning the disclosure or use of information. Accordingly, VA employees and contractors must comply with the following responsibilities when handling sensitive personal information:

- Accessing records containing PII only when the information is needed to carry out their official duties.
- Disclosing PII about veterans, employees, contractors, volunteers, interns, and business associates only in accordance with applicable federal privacy laws, regulations, and VA policies and procedures.
- Taking privacy awareness training provided or approved by the VA Privacy Service on an annual basis.
- Taking any role-specific privacy training provided or approved by the VA Privacy Service that is applicable to their official duties.
- Reporting all actual or suspected breaches involving PII to their privacy officers within one hour of discovery.

According to VA Handbook 6500.2, *Management of Breaches Involving Sensitive Personal Information*, a breach refers to the potential acquisition, access, use, or disclosure of VA sensitive information in a manner not permitted by law or VA policy that compromises the security or privacy of the information. If the acquisition, access, or use

of sensitive personal information by a VA workforce member is unintentional and does not result in the further use or disclosure in a manner not permitted by law or VA policy, or when there is a low probability, the information has been compromised, it is not a breach.

VA Handbook 6500.2 also establishes procedures for managing breaches. Subject to the handbook procedures, VA's Data Breach Response Service determines whether the reported event constitutes a breach that must be reported to the Department of Health and Human Services under the HIPAA Breach Notification Rule, and whether VA will notify the involved individuals of the event and offer them credit protection services.

Privacy Threshold Analysis

A Privacy Threshold Analysis (PTA) is used to identify IT systems, rulemakings, programs, or pilot projects that involve Sensitive Personal Information (SPI) and other activities that otherwise impact the privacy of individuals as determined by the Director, Privacy Service, and to assess whether there is a need for a Privacy Impact Assessment (PIA), whether a System of Records Notice is required, and if any other privacy requirements apply to the IT system. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, or other Department activity and describes what SPI is collected (and from whom) and how that information is used. The PTA is considered to be a key element in an IT system's Authorization and Accreditation (A&A) process.

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is used to analyze how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. A PIA is required to be performed in the conceptualization phase of the system lifecycle and updated whenever a system change could create a new privacy risk and is considered to be a key element in an IT system's A&A process.

VI. Findings, Conclusions, and Recommendations

Allegations 1 and 2

These allegations are addressed together due to their similarity.

1. *VA officials 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.*

2. *VA officials have failed to protect the confidentiality of veterans' PII in VIEWS, in violation of federal law and agency directive and handbook provisions.*

Findings

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 had been directed to run a search of files relating to the whistleblower and that all files located had been made sensitive. The DEPCOSVA also stated that the request to investigate the whistleblowers' allegations was received from the Office of Special Counsel (OSC) during this same timeframe, and that communications with the whistleblowers ceased so as to not interfere with that investigation.

Inherent Privacy Protections and Accessibility of Sensitive Personal Information and Whistleblower Identification in VIEWS CCM

VIEWS CCM was intentionally designed to securely manage sensitive personal information. Besides the many cyber protections that are transparent to most system users, the presence of a case sensitivity indicator provides access restrictions for cases containing sensitive personal information. Restricting access to a case is as simple as the case owner selecting "Sensitive" from the dropdown menu in the case information section. When a case has been marked "Sensitive," only the case owner and explicitly identified users can open the case and view its contents. Some associated fields remained searchable and viewable until very recently though, such as the case title and description. The successfulness of this function primarily rests on the diligence of the case owner and related case users. Failure to appropriately mark a case sensitive allows the contents to be viewable by anyone with an active VIEWS CCM user account. Users assigned to work an inappropriately marked case can perpetuate the problem by uploading sensitive documents or making sensitive annotations in the case notes. VIEWS CCM provides strong search functionality that can generate a portfolio of results with just a few keystrokes, making finding information related to specific people, topics, and organizations fast and simple. While this is a highly desirable capability when used

for authorized purposes, it is a significant enabler for those who are intent on gathering sensitive personal information.

Prior to recent remediation actions, searches of VIEWS CCM by a user, using terms such as "whistleblower", "complaint", and various forms of "date of birth", "DD214", and "social security number", returned numerous "Not-Sensitive" cases with visible names and personal information of whistleblowers and people making complaints against the VA or named VA employees, as well as sensitive personal information of Veterans and 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.

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.

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.

Obstacles to Addressing and Remediating Mishandling of Sensitive Personal Information in VIEWS CCM

Lack of Ownership and Accountability. Officials from the Executive Secretariat responsible for the management of VIEWS CCM have stated that responsibility for proper handling of sensitive personal information in VIEWS CCM rests with VIEWS users, and that policy and required training are adequate to inform the user of this

responsibility. Yet based on the many VIEWS CCM cases incorrectly marked as not sensitive found during the investigation prior to the recently implemented changes, policy and training alone have not been effective in ensuring users managed sensitive personal information appropriately; nevertheless, there has been no effort to hold violators accountable.

Negative Impact to Business Operations. The nature of correspondence and cases requiring senior VA leadership attention are such that required actions and responsible stakeholders cannot always be immediately determined. VIEWS CCM supports the assignment of individuals and teams of individuals to a specific case. Person(s) assigned to a case marked "Sensitive" have access to the contents of that case, while unassigned users do not. A case marked "Sensitive" requires greater care when assigning individuals and teams to a case, as missing a key stakeholder could cause a work stoppage until the issue is detected and resolved. Considering that an average of 260 cases are initiated in VIEWS CCM every business day, these delays could have significantly negative consequences to VA's responsiveness in a wide spectrum of business functions.

Level of Effort Required to Remediate Existing Cases. Although the true number of cases that might require a change in case sensitivity was unknown prior to the recently implemented changes, it was expected that hundreds of thousands of cases would need to be opened and assessed. In addition, cases determined to be sensitive would require case membership to be validated for access by authorized users. This would be a very labor-intensive project, potentially requiring thousands of manhours to complete.

User Accountability. Managers have stated that since VIEWS CCM users have received system-specific and annual privacy training and see a warning banner when logging into VIEWS CCM, they understand that they are responsible for not viewing sensitive personal information for which they have no business need, regardless of their ability to view such information.

VA's Activities to Protect Sensitive Personal Information in VIEWS CCM

Privacy issues with VIEWS CCM have been reported to VA officials responsible for VIEWS CCM by multiple persons and offices since 2019.

In July 2019, as revealed in heavily redacted documents obtained from the VA Office of General Counsel (OGC), an OGC Deputy Chief Counsel alerted the Executive Secretariat of privacy concerns related to VIEWS CCM. Interviews of persons involved in the management, operation, and sustainment of VIEWS CCM identified these concerns as the practice of using the system's integrated "Chatter" function to share sensitive personal information, which was at the time viewable by all users, and the ability of all users to view sensitive personal information in a massive number of cases that were improperly marked "Not Sensitive." The Executive Secretary, as the VIEWS CCM Business Owner, engaged OIT leadership and SMEs to validate the concerns and determine resolutions. As a result, system enhancements and changes in policy and training were implemented in 2019 and 2020. Amongst these were the disabling of the

"Chatter" function, targeted training of users from the Veterans Experience and Whitehouse Hotline offices, the addition of a case sensitivity section to one of the four mandatory online user training courses, and the placement of a system warning banner on the Salesforce (VIEWS CCM host platform) login script. Although the redacted emails indicate that significant resources were mobilized to address the reported privacy concerns, there are no indications that a deliberate process was employed to assess and determine appropriate mitigations, or to measure the effectiveness of the actions that were taken.

In July 2022, two VA whistleblowers informed a VA Deputy Chief of Staff (DEPCOSVA) via email of their concerns with the security of sensitive information contained in VIEWS CCM. The whistleblowers alleged that any VIEWS CCM user was able to search for and view full social security numbers, dates of birth, home addresses, and other sensitive information about Veterans and employees. Additionally, they alleged that searches for "OAWP," "OSC," "whistleblower," "dispute," "complaint," "congressional," and other such terms would generate many thousands of results containing detailed information about VA employee whistleblower retaliation complaints, thus making those complaints potentially accessible to the very people who were alleged to have committed wrongdoing. In August 2022, the whistleblowers again contacted the DEPCOSVA and expressed concerns about their own sensitive personal information not being protected in VIEWS CCM, and how a search of their names resulted in a compilation of all whistleblower records and activities associated with them, to include sensitive personal information. In both cases the DEPCOSVA acknowledged receipt of their concerns and stated that the matter would be looked into. No further correspondence from the DEPCOSVA was received by the whistleblower. The DEPCOSVA may have ceased communications with the whistleblowers so as to not interfere with this subsequent investigation that had been initiated at OSC's request. It also should be noted that on August 29, 2022, at the behest of DEPCOSVA, the business owner directed OIT's Data Transformation Center (DTC) to "change all cases about [the whistleblower's name] from Non Sensitive to Sensitive." DTC reported back that 2 cases with the whistleblowers' name were found; one was sensitive and the other was "updated to sensitive per this request." It is not clear why DTC did not identify other cases involving the whistleblowers that had been incorrectly marked as not sensitive.

Also in July 2022, one of the whistleblowers notified the VA Privacy Service that they had been informed by an anonymous source that there were 10 cases in VIEWS CCM containing their personal information and that this information was not secured and was available to anyone with VIEWS CCM user access. The VA Privacy Service investigated and determined that the report was valid, although the investigation concluded only five of the cited cases actually contained sensitive personal information, and that these files had only been accessed by authorized employees for official reasons, with one exception: an employee who was no longer employed with VA and whose authorization to access the files could not be validated. The VA Privacy Service's response to the whistleblower via formal letter did not disclose if the reported issue had been remediated. As part of this investigation, the cases cited in the report were reviewed and found to now be marked "Sensitive", making them no longer viewable by users who were not assigned to the case team. The review also discovered a new "Not

Sensitive" FOIA request case initiated in August 2022, which was shortly after the Privacy Service investigation was concluded, containing the whistleblower's date of birth, social security number, address, and phone number. As discussed below, because of the recent changes to VIEWS, this FOIA request case is now marked as "Sensitive" and therefore is no longer accessible to VIEWS CCM users.

In September 2022, the VA Executive Secretary briefed the House Committee on Veterans Affairs (HVAC) on VIEWS CCM. The catalyst for the briefing is undetermined, but the timing and subject matter of the request make it likely to have been the result of disclosures made to the HVAC by whistleblowers whose sensitive personal information, provided as part of a request for congressional assistance, were discovered to be viewable by VIEWS CCM users. As a follow-up to the brief, the HVAC requested responses to seven questions regarding VIEWS CCM users, training, case sensitivity, processes, and policy. The Executive Secretary drafted the responses with the assistance of OIT SMEs, which also included the following list of security improvements to be completed or deployed by 2nd quarter FY23.

- Case Sensitivity would be a required field for all new VIEWS CCM cases.
- Case Sensitivity would be limited to two options: (1) Sensitive, and (2) Not Sensitive.
- A new field, "Pending Review," would be created on the VIEWS CCM Case Object, and it would have two options: (1) Yes, and (2) No. The new field would be optional for those Case Record Types "Congressional Correspondence" and "White House VA Hotline Non-Complaint," and potentially others to be determined during a subsequent business requirements analysis.
- VIEWS CCM and White House VA Hotline new user training would be updated to provide further guidelines on the use of the Sensitive Case and Pending Review fields.
- An announcement would be sent via email to all current VIEWS CCM and White House VA Hotline users concerning the use of the Sensitive Case and Pending Review fields.

These measures to improve protections for sensitive personal information in VIEWS CCM were all implemented by the managers of VIEWS. Additionally, the VIEWS Business Owner and IT Program Manager began researching data scanning tools capable of identifying user-defined information handling scenarios as a means of detecting suspicious behavior. Such tools could augment system enhancements by locating sources of policy violations that could then be addressed through enforcement and remediation actions.

In December 2022, a second whistleblower notified the VA Privacy Service that their own sensitive personal information, to include prior whistleblower activities, was also unsecured in VIEWS CCM. The whistleblower chose to not use the standard process for reporting privacy violations, which was to send an email to the Privacy Service's shared email address, because of a fear that this could expose their prior whistleblower

activities to people in their current workplace. For example, someone from the Privacy Service might contact the whistleblower's supervisor to discuss the details of their report, thereby disclosing that they were a former whistleblower, the details of which could then be viewed by the supervisor in VIEWS CCM. Instead, they initiated the report with a voice message to one of the senior Privacy Service managers. Approximately five months after initially reporting their concerns, and only after requesting a status of their report, they received an email stating that the VIEWS program office (i.e., the Executive Secretariat) related that their information would only be accessed by VIEWS CCM users with a verified need to know, and that the Privacy Service could request an access audit if they (the whistleblower) felt their information had actually been accessed by unauthorized persons. As of the date of this report, the whistleblower's information is still viewable by any VIEWS CCM user.

In June 2023, the Executive Secretary issued a memorandum titled "Additional Department of Veterans Affairs (VA) Integrated Enterprise Workflow Solution Security Processes." The memo implemented a vetting process for prospective VIEWS CCM users and provided three qualification criteria. Also included was notice that any account without activity for 45 days would be subject to deactivation, which was a change from the previous 90-day threshold. Additionally, the memo reminded users of their responsibility to only access cases necessary for completing job-related tasks, and of the potential consequences of unauthorized activities. The memo also advised that user training would soon become an annual requirement.

As part of this investigation, a review of actions taken to improve VIEWS CCM security and protection of sensitive personal information was conducted. The review revealed such actions had or would have limited effectiveness. Specifically:

- The forced use of case sensitivity defaults to "Not Sensitive" for new cases. Since there is no requirement or prompt for the user to make a sensitivity decision during the case initiation process, cases are likely to remain "Not Sensitive" regardless of contents.

- Revisions made to user training specifically address case sensitivity, but current users would not be required to take retraining until a later date.

- The forced use of case sensitivity does not apply to information contained in, or appended to, cases already in the system prior to when the change was implemented.

- The disabling of the "Chatter" function did not remove visibility of historical posts containing sensitive personal information.

- An aggressive program of user vetting and validation will likely result in fewer users, which could potentially reduce the volume and frequency of privacy violations, but it would not eliminate the fundamental issue of every user having unrestricted access to cases containing sensitive personal information regardless of their need-to-know if the case was previously improperly designated as "Not Sensitive."

In June 2023, an assessment of the effectiveness of updates reported as having been completed to-date was conducted in the form of key term searches performed by a VIEWS CCM user. It indicated that these updates were ineffective in protecting sensitive personal information from unauthorized access by a VIEWS CCM user in those cases where users had not appropriately marked the case as sensitive. Each search returned many cases containing sensitive personal information. Below are representative results:

- A search for "complaint" returned a copy of a June 16, 2023, email from a named Veteran / VA employee (i.e., whistleblower) titled "Seeking help against Leadership for unfair treatment..." in an Office of Congressional and Legislative Affairs and Veterans Health Administration "Not Sensitive" case.
- A search for "DD214" returned a copy of a June 8, 2023, email with an attached military records request form containing a Veterans social security number, date of birth, home address, and other identifying information, in an Office of Congressional and Legislative Affairs and Veterans Benefits Administration "Not Sensitive" case.
- A search for "SSN" returned a copy of an April 7, 2023, email from a congressional staffer with a Veteran's social security number in a VA Office of Congressional and Legislative Affairs and Board of Veterans Appeals "Not Sensitive" case.
- A search for "DOB" returned a copy of a March 3, 2023, "Ask VA" intake form with a Veteran's full social security number, date of birth, and service dates in a National Cemetery Administration "Not Sensitive" case.
- A search for "whistleblower" returned a copy of a February 21, 2023, email from a named VA employee claiming to be the subject of whistleblower retaliation in a Congressional and Legislative Affairs and Office of Whistleblower Protection (OAWP) "Not Sensitive" case.

However, more recently, the business owner has taken additional remedial actions addressing both past and future cases which appears to have dramatically reduced improper access to sensitive information. Further, the VIEWS IT Program Manager shared a corrective action plan that addressed VIEWS CCM privacy and security vulnerabilities. The plan was coordinated with subject matter experts, to include the Privacy Officer and Information Systems Security Officer (ISSO) and contained 31 technical system updates and several non-technical actions, such as the evaluation of published training materials and privacy assessments. The plan was divided into three phases: Phase 1 was titled "Secure VIEWS Database" and contained 17 updates related to case sensitivity; Phase 2 was titled "Implement Governance Oversight for VIEWS" and contained one technical action related to the development of sensitive personal information scanning capabilities in VIEWS, Phase 3 was titled "Ongoing Support EXECSEC Governance and Oversight Program for VIEWS" and contained 13 updates and other miscellaneous activities that could further enhance the security of VIEWS. The plan indicated that the17 Phase 1 technical updates had been completed between the dates of June 29, 2023, and July 20, 2023.

A functional assessment of these updates, conducted in the form of key term searches and sample case initiation performed by a VIEWS CCM user, indicated that these updates were largely effective in securing existing and new cases from unauthorized access. For example, we re-performed the same searches done in June 2023, and none of the documents with sensitive personal or whistleblower information described above were returned. However, we noted the following exceptions:

- Searches using the term "SSN" and "complaint" resulted in cases regarding Veteran complaints and inquiries into benefits and healthcare, many of which contained sensitive personal information in the form of social security numbers, details of benefits, and protected health information in case notes and attachments. These were cases without a case sensitivity indicator or an indicator of "Pending Review".
- The Veterans contacts database was still viewable. This database contains full names, dates of birth, and home addresses and phone numbers of Veterans, and can be accessed from a case linked to the Veteran or directly using the VIEWS CCM menu.
- Files were found containing sensitive personal information without an associated case number and therefore no sensitivity indicator that would define viewability.

System Access Logs and Auditing

VIEWS CCM has an integrated logging capability that displays changes made to case information and changes made by users, but it does not capture instances where a user simply viewed case information or downloaded files.

Case and file access history was requested from the OIT Data Transformation Center (DTC), which has responsibility for sustaining VA's Salesforce platform and related security and networking systems, and which has previously provided audit reports in support of privacy act violation investigations. The DTC possesses specialized data tools that should be capable of generating audit reports, but when requested, the DTC was unable to produce a report that contained information beyond what was already available within the application's integrated capability. As an explanation, the assigned DTC solution architect shared that the recent transition to a new data tool was impacting their ability to produce usable audit reports.

As such, even though we were able to substantiate during our investigation that there were incorrectly marked cases where users could easily access sensitive personal information without authorization, we were unable to assess the frequency of such unauthorized access, or even if such access had ever occurred. Additionally, in light of this auditing limitation, 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).

The corrective action plan provided by the VIEWS IT Program Manager on July 21, 2023, includes plans for the creation of an audit log for case sensitivity changes and a feasibility analysis for auditing PII/PHI in VIEWS.

Authority to Operate and Associated Assessments and Plans

Historical (inactive) assessment and approval records were not available in the Enterprise Mission Assurance Support Service (eMASS), which is the VA's central Governance, Risk and Compliance tool for IT systems.

Current records identify that in March 2021, a VA Enterprise Authority to Operate (ATO) was issued for VIEWS CCM's host platform, Salesforce Government Cloud Plus (SFGCP). Neither a Privacy Threshold Analysis (PTA) nor a Privacy Impact Assessment (PIA) were required or completed in preparation of VIEWS CCM going live in 2018.

As of October 2020, the VA Minor Application Security Assessment process did not require an ATO for VIEWS CCM but did require the completion of a PTA. VA IT procedures did not require a dedicated ATO for a minor application possessing a Federal Information Processing Standard (FIPS) 199 Security Categorization of Low or Moderate, that was hosted on a parent platform possessing a valid ATO. VIEWS CCM has a FIPS 199 categorization of Moderate. Depending on the results of the PTA, the process may require that a PIA be completed.

In August 2021, a PTA and a PIA were completed for VIEWS CCM.

In June 2022, a notice of a modified system of records for VIEWS CCM was published in the Federal Register. This notice makes no mention of the collection or storage of sensitive personal information in the system, although it states that social security numbers and other unique identifiers are used to retrieve records contained in the system. The notice also states in the Administrative, Technical, and Physical Safeguards section that "Access to records is limited to those employees who require the records to perform their official duties consistent with the purpose for which the information was collected," which is inaccurate since VIEWS CCM users were not truly limited from accessing sensitive personal information contained in cases not marked "Sensitive."

In September 2022, new PTA, PIA, and supporting security and system risk assessments and plans were completed for VIEWS CCM. Inconstancies and omissions regarding the protection of sensitive information were discovered in these documents.

- The PTA and PIA both stated that social security numbers (SSN) were retrieved only from the Master Person Index (MPI) and the Identity Access Management Access Services System (IAM ACS) to verify identity and credentials. The PTA did not identify the SSN as a collected data element, whereas the PIA stated that the last four digits of the SSN were retained. The PIA specifically stated, as a risk mitigation, that "No personal data is collected directly from individuals.", where in fact, instances can be found in VIEWS CCM where a user corresponded directly with an individual to collect their full SSN and then posted that SSN in a "Not Sensitive" case file.

- The PIA identified several privacy risks associated with the exposure and release of personally identifiable information to unauthorized individuals. Mitigations provided for these risks were misleading and failed to fully address the entirety of the risk. As an example, the mitigation for the risk "*SPI, including personal contact information, SSN and medical information, may be released to unauthorized individuals*", stated in part that "*Profile-based permissions govern user access to information. The profiles are reviewed on a regular basis to ensure that information is shared only with appropriate users.*" In fact, every VIEWS CCM user had unrestricted access to every case (and its associated information) in VIEWS CCM, unless that case had been marked "Sensitive." The ability to access information was not profile-based, and a review of profiles would have provided no mitigating affect to this risk.

- The PTA, PIA, and supporting security and system risk assessments did not acknowledge whistleblower identification as being received, collected, or stored in VIEWS CCM, or as a discreet data element requiring special protection.

Conclusions

- We **substantiate** that, although they have undertaken substantial efforts and made considerable strides in improving the protection of sensitive information in VIEWS, VA officials still need to take additional measures to protect the confidentiality of whistleblower identities, their submissions, and PII in VIEWS CCM, as well as the confidentiality of veterans' PII in VIEWS, to ensure against violations of the Privacy Act, the Whistleblower Protection Act and VA Directive 6502.

- The system business owner was aware that there likely were a significant number of cases containing sensitive personal and whistleblower information that were not appropriately marked and not protected from unauthorized access by system users. The business owner noted that given the large volume of cases and thousands of VIEWS users, it was inevitable that some users had not marked cases appropriately, contrary to their training and VA policy.

- Following the issues about sensitive information in VIEWS CCM being first raised by whistleblowers, the system business owner took steps to improve and remediate privacy issues. However, some users did not appropriately mark cases that contained personal, PII or whistleblower information as sensitive. In those cases where the case users have not appropriately marked a case as sensitive, VIEWS CCM users are allowed access to this sensitive personal or whistleblower information without respect to their functional role and real or potential need to access such information.

- More recently, changes applied to VIEWS CCM in July 2023 significantly reduced the accessibility of whistleblower identities and sensitive personal information contained in archived and active cases, by mass converting designated case types to "sensitive," and reconfiguring system business rules for case type and case sensitivity.

- System users can still search for and view whistleblower identities and sensitive personal information, although to a much less degree, found in cases with blank or "Pending Review" case sensitivity indicators, in disassociated case files, and in the Veterans contacts database. This ability is not restricted to a user's functional role or need to access such information.
- 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 assessment processes employed to authorize the operation of VIEWS CCM, although in compliance with VA IT policy, failed to meet the objective of identifying and mitigating privacy and security risks associated with the use of sensitive personal information. The practice of referring security assessments for minor applications to parent applications, although expedient, may have led to the failure of the identification and mitigation of privacy vulnerabilities unique to VIEWS CCM.
- The VA Privacy Service failed to appropriately respond to and remediate a privacy incident reported by a whistleblower. The Service's response, as monitored throughout the period of this investigation, was not timely and provided incorrect information to the whistleblower regarding the accessibility of files in VIEWS CCM containing their identity, whistleblower activities, and sensitive personal information. Additionally, the response was inconsistent with that of a previous near identical report made by another whistleblower where an appropriate process was followed.

Recommendations to the VA Office of the Executive Secretariat

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.

    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.

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.

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.

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.

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.

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

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

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.

Recommendations to VA Privacy Service

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.

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

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.

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.

Recommendations to VA Office of Information and Technology

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

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 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.

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.

Allegation 3

VA officials have failed to include VIEWS in FOIA and Privacy Act requests, in violation of federal law and agency directive and handbook provisions.

Findings

When asked, the VA FOIA Office was able to quickly identify at least three recent cases where VIEWS CCM was searched, and material was reviewed for relevancy and ultimately released to the requester. FOIA Officers are required to conduct and document searches reasonably calculated to produce records relevant to a request. Because of this standard, if a request has a VIEWS CCM nexus, the FOIA Officer will search VIEWS CCM, document that search, review any relevant records, and make a release determination.

When asked, the VA Privacy Service was unable to provide any specific cases in which VIEWS CCM had been searched in response to a Privacy Act request but stated that Privacy Act requests were received and independently acted upon by offices across VA,

and that there was no central database that could be searched for requests involving VIEWS CCM.

Conclusions

- We were **unable to substantiate** that VA officials have failed to include VIEWS in FOIA and Privacy Act requests, in violation of federal law and agency directive and handbook provisions.

Recommendations

There are no recommendations specific to this allegation.

Allegation 4

VA Police use VIEWS as a source information for people who are being investigated for suspected criminal activity, in violation of federal law and agency directive and handbook provisions.

Background

During interviews of witnesses, we found that this allegation stemmed from a belief that the Disruptive Behavior and Reporting System (DBRS), implemented as a part the Veterans Health Administration Workplace Violence Prevention Program (WVPP), was linked to VIEWS CCM making VIEWS CCM information viewable by VA Police.

Findings

SMEs for VIEWS CCM confirmed there were no data connections between DBRS and VIEWS CCM.

Conclusions

- We were **unable to substantiate** that VA Police use VIEWS as a source information for people who are being investigated for suspected criminal activity, in violation of federal law and agency directive and handbook provisions.
- VA Police do not access information in VIEWS CCM through a DBRS interface, as such an interface does not exist.
- Only seven VA Police offices have VIEWS CCM access; each of these offices has a single employee as a VIEWS CCM user.
- Without the ability to conduct comprehensive audits of VIEWS CCM user activity, it is not possible to determine if VA Police view and utilize VIEWS CCM as a source of investigative information.
- It is undetermined if such use would violate any laws, rules, or policies.

Recommendations

There are no recommendations specific to this allegation.

VII. Summary Statement

VA developed this report in order to address whistleblower allegations that VA officials had failed to protect the sensitive personal information of whistleblowers, Veterans, and employees stored in the agency's case and correspondence management system (VIEWS CCM). We reviewed the allegations and determined the merits of each.

We **substantiate** that, although they have undertaken substantial efforts and made considerable strides in improving the protection of sensitive information in VIEWS, officials from the Office of the Executive Secretariat still need to take additional measures to protect the confidentiality of whistleblower identities, their submissions, and PII in VIEWS CCM, as well as the confidentiality of veterans' PII in VIEWS, to ensure against violations of the Privacy Act, the Whistleblower Protection Act and VA Directive 6502. We found that the system by design is capable of protecting sensitive personal information through the use of case sensitivity indicators, but that the use of this capability had not been monitored or enforced by managers, resulting in thousands of cases containing sensitive personal information not being fully protected from unauthorized disclosure because of users failing to appropriately mark cases as sensitive. When learning of this vulnerability in 2019, managers took actions that provided limited improvements in policy and technical protection but did not act to ensure correct utilization of the system's security capabilities or remediate the unprotected sensitive cases, choosing instead to rely upon users following policy and refraining from viewing information for which they had no authorization to view. Managers primarily based this decision on the relatively low number of system users, the excessive resources they expected to be needed to implement effective corrective actions, and the concern that remediation and enforcement activities would result in work stoppages in critical business functions. Recent corrective actions have significantly reduced the accessibility of whistleblower identities and sensitive personal information contained in archived and active cases. However, system users can still search for and view such information without authorization, although to a significantly lesser degree, in the Veteran contacts database and in cases and files still pending remediation.

We were unable to substantiate that VA officials have failed to include VIEWS in FOIA and Privacy Act requests, or that VA Police use VIEWS as a source of investigative information.

Attachment A

The following documents and systems were reviewed:

VA Directive 6502, VA Enterprise Privacy Program, May 2008.

VA Handbook 6500, Risk Management Framework for VA Information Systems and Information Security Program, February 2021.

VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, October 2014.

VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment, July 2015.

VA Directive 6509, Duties of Privacy Officers, July 2015.

VA Directive 6213, Freedom of Information Act (FOIA), September 2021.

Whistleblower Protection Act.

Inspector General Act of 1978.

The Privacy Act of 1974.

The Freedom of Information Act.

The Health Insurance Portability and Accountability Act of 1996.

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources.

OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 2007.

Title 38 United States Code -Section 5701, Confidential Nature of Claims.

Minor Application Assessment Requirements for Enterprise Mission Assurance Support System (eMASS) Standard Operating Procedure, August 2022.

Product Outcome Roadmap (VIEWS CCM), February 2023.

Privacy Impact Statement (Salesforce-VIEWS CCM), September 2022.

System of Records Notice (SORN) (VIEWS CCM), June 2022.

System Security Plan (VIEWS CCM), August 2023.

Security Assessment Report (SAR) (VIEWS CCM), August 2022.

System Risk Assessment Report (VIEWS CCM), August 2022.

VA Systems Inventory Report (VASI) (VIEWS CCM), November 2022.

VA Systems Inventory (VASI) Detailed System Report (VIEWS CCM), November 2022.

Use Cases and Change Log (VIEWS CCM), February 2023.

Managing Cases in VIEWS CCM training, October 2022.

Introduction to VIEWS CCM training, Undated.

VIEWS Case and Correspondence Management for Leaders training, Undated.

Working with Case Tasks in VIEWS CCM training, Undated.

Privacy Threshold Analysis and Privacy Impact Assessment Training, March 2023.

New User Guide for All Users (VIEWS CCM), November 2020.

Featured Functionality: VIEWS Congressional Correspondence Case Sensitivity, Undated.

Notification Letter, Privacy Incident Investigation, July 2022.

Office of the Executive Secretary Memorandum (104781133): Additional VIEWS Security Processes, June 2023.

VA Office of the Inspector General Audit Report (VAOIG-20-00178-24): Program of Comprehensive Assistance for Family Caregivers: IT System Development Challenges Affect Expansion, June 2021.

VA Office of the Inspector General Audit Report (VAOIG-19-06125-218): Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives, October 2019.

VIEWS CCM Corrective Action Plan

Statements provided by staff.

Redacted emails provided by the Office of General Counsel (OGC).

VIEWS CCM Search Results.

Emails provided by staff.