United States Senate
WASHINGTON, DC 20510

June 2, 2023

VIA ELECTRONIC TRANSMISSION

The Honorable Denis R. McDonough
Secretary
Department of Veterans Affairs

Dear Secretary McDonough:

I have received legally protected disclosures from multiple credible whistleblowers that VA has mishandled sensitive, private information in the VA's Integrated Enterprise Workflow Solution (VIEWS) system, the system VA uses to manage and track its correspondence. This system, as you know, contains sensitive personal information on countless veterans, VA employees, inquiries from members of Congress, and even VA whistleblowers. The VIEWS system is under the authority of Chief of Staff Tanya Bradsher's office.[1] Based on reports that are supported by documents in my possession, a VA certified fraud examiner and certified auditing professional notified Ms. Bradsher's office last year that personal identifiable information (PII), protected health information (PHI), and whistleblower information was widely accessible across VA to the thousands of VA employees with access to VIEWS, regardless of their need to know.[2] The whistleblower also alerted the Office of Special Counsel (OSC) of this potential data breach. In response, OSC found a "substantial likelihood of wrongdoing," including potential violation of federal privacy laws.[3] OSC then ordered VA to investigate the matter, which it asked be completed within 60 days.[4] According to these whistleblowers, the data vulnerabilities are still present in the VIEWS system and threaten the privacy of countless people who trust the VA to safeguard their private information, including members of Congress who pass sensitive constituent information to the agency.[5]

---

[1] Liberty IT Solutions (the company that implemented the VIEWS system at VA), summary, VA integrated Enterprise Workflow Solution (VIEWS) Salesforce Development (last accessed May 31, 2023), https://appexchange.salesforce.com/partners/servlet/servlet.FileDownload?file=00P3A00000iHXXiUAO (noting that while operationally, correspondence management falls under the Office of the Secretary of the VA (OSVA) Secretariat (ExecSec), the VIEWS system is under the authority of the Chief of Staff).

[2] Email from Peter Rizzo, Senior Program Manager, Quality Assurance Service, Office of Construction & Facilities Management, U.S. Dep't of Veterans Affairs, to Ms. Maureen Elias, Deputy Chief of Staff, July 13, 2022, on file with Committee staff.

[3] Letter from Leslie J. Gogan, Attorney, Disclosure Unit, Office of Special Counsel, to Mr. Peter Rizzo (August 2, 2022), on file with Committee staff.

[4] *Id.* (citing OSC's legal authority under 5 U.S.C. § 1213(c)).

[5] Documents showing apparently sensitive information still marked not sensitive as of June 2023 in the VIEWS system are on file with Committee staff.

According to documents in my possession, the VIEWS system is hosted on the Salesforce platform.[6] However, VA's Inspector General in an audit report in 2021 noted sensitive information such as PHI should not be hosted on Salesforce, a moderate-risk cloud environment, but rather on a cloud environment rated for high risk.[7] The IG reported that the VA did not properly consider the risk to PHI it hosted on a different VA software system that also operated on the Salesforce platform. VA needs to explain why it continues to host sensitive information on this system. It appears from the OIG's report that even if the proper sensitivity tags were being applied, which is not the case, the system still would not be appropriate to store this sensitive information.

According to whistleblowers, the VA has requested extensions from OSC that have left its report on this serious matter still unfinished ten months after OSC ordered VA to investigate. As you know, Ms. Tanya Bradsher, whose office has authority over the VIEWS system and promised to look into the matter nearly 11 months ago, is currently before the Senate as a nominee to the position of Deputy Secretary. In that position, she would have a key role in the VA's electronic health records (EHR) modernization.[8] However, the VIEWS system that is under her authority contains names, social security numbers, dates of birth, and apparently even medical records of many veterans, accessible to thousands of VA employees and not restricted to those with a direct need to know.

VA and Ms. Bradsher must immediately explain their failure to protect this information for so long, even after being notified of these potential violations of federal data privacy laws. VA must also explain its delays in investigating the matter, while this sensitive information apparently remains available to those who should not have access to it. Accordingly, so that Congress may conduct thorough and independent oversight of the VIEWS system and what appears to be a major breach of the public trust by Ms. Bradsher's office and senior leadership at VA, please provide the following information no later than June 16, 2023:

1. All records[9] sufficient to show when VA first became aware of potential issues with the security of VIEWS data, including all correspondence following notification of the Chief of Staff's Office in 2022 about vulnerabilities in the VIEWS system.

2. All records related to data vulnerabilities in the VIEWS system, including any forensic or other analysis of how the information was used, potential access by those without a need to know, potential misuse of VIEWS information, and potential use of information for

---

[6] Liberty IT Solutions, *supra* n. 1.
[7] Dep't of Veterans Affairs, Office of Inspector General, Office of Audits and Evaluations, Veterans Health Administration, Program of Comprehensive Assistance for Family Caregivers: IT System Development Challenges Affect Expansion, Report #20-00178-24 (June 8, 2021), https://www.va.gov/oig/pubs/VAOIG-20-00178-24.pdf.
[8] Dep't of Veterans Affairs, EHR Modernization (last accessed May 31, 2023), https://digital.va.gov/ehr-modernization/.
[9] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (e-mails, email attachments, and any other electronically-created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether or not they resulted in final documents).

whistleblower retaliation.

3. All policies and procedures for when information in VIEWS should be marked sensitive, PII, or PHI, and restricted from dissemination within VA.

4. All records related to the investigation requested by OSC, including any and all correspondence related to delays in the report.

5. Any records or correspondence showing Ms. Bradsher's role in overseeing the VIEWS system, including any emails, memoranda, or other instances where she instructed anyone at VA to follow up on reports of data vulnerability in the system.

6. Provide in detail all steps Chief of Staff Bradsher took when she was notified of this major data vulnerability in 2022, along with records detailing and documenting each step.

If you have any questions, please reach out to James Layne, on my Committee staff, at (202) 224-0642.

Sincerely,

Charles E. Grassley
Ranking Member
Committee on the Budget

Cc: The Hon. Michael J. Missal
Inspector General