Senator Blackburn
Questions for the Record
Senate Veterans' Affairs Committee
Hearing To Consider the Nomination of Tanya J. Bradsher to be Deputy Secretary, Department of Veterans Affairs
May 31, 2023

Questions for Nominee Bradsher:

1. **Given that the EHRM contract extension is now in place and appropriately increases vendor accountability with significant increases in penalties and the addition of over twenty contractual service obligations, do you feel that the accountability on VA needs to be equally increased?**

   If confirmed, I am committed to transparency and excellence in the EHR implementation, and that commitment includes increased accountability on VA to get this right. As the Secretary has said on numerous occasions, this is not a can do—this is a must do. VA will continue to engage congressional and other stakeholders with full and proactive transparency on VA's progress on the EHRM program. I value congressional oversight in holding VA accountable as we work to advance the access, outcomes, and excellence that Veterans deserve.

   a. **Will you commit to driving equal accountability and transparency into VA?**

      Yes, if confirmed I am fully committed to driving equal accountability and transparency into VA. My leadership approach involves going out, boots on the ground, to all five sites to do listening sessions with our clinicians. We have the opportunity with the EHRM program reset to make sure that we're able to incorporate those recommendations enterprise-wide. And ensure that we hold Oracle Cerner accountable to make sure those changes happen, and make sure we can scale to large facilities when deployments resume.

   b. **If confirmed, what metrics would you put on VA to ensure accountability on your end?**

      With the completion of the renegotiated Oracle Cerner contract, I am encouraged by what I see as an increase in VA's ability to hold the vendor accountable across a variety of key areas, including reliability (minimizing outages), responsiveness (quickly and reliably resolving tickets), interoperability with other health care systems, and interoperability with other applications. If confirmed, I would drive VA to apply these same areas of accountability within our own enterprise. One example of this is with incident free time. VA has a goal of at least 95% incident free time—we have not yet met that goal but are moving in the right direction.

c. **What changes would you make internally to drive accountability within VA?**

For the past few years, we have not delivered the results that Veterans deserve. This reset changes that. I am committed to making sure we are not going to continue deployment activities at future sites during the reset; instead, we are going to take the time necessary to get this right for Veterans and VA clinicians alike, and that means focusing our resources solely on improving the EHR at the sites where it is currently in use and optimizing the fit of the EHR for VA more broadly. If confirmed, I would continue to focus on standardizing activities across VHA to optimize business processes, reduce user adoption issues and improve training and testing.

2. **With an enterprise system, not all end-users and sites will be able to get what they would like in terms of changes. Currently, VA is good at compiling the feedback, but no one seems to be working through the lists to see if proposed changes are in fact needed or are consistent with not customizing the system and creating another VistA.**

a. **If confirmed, who in VA should be accountable for making and enforcing enterprise decisions and saying no to specific site customizations?**

First and foremost, the Deputy Secretary is ultimately responsible for the EHR. If confirmed, that responsibility will fall on my shoulders. VA has to ensure that our Veterans get the record they need. VA clinicians have not seen the results of their comments come back and be executed within the EHR. VA has the opportunity with the reset to make sure that we are able to incorporate those recommendations enterprise-wide, because we can’t have five different records. VA needs to implement enterprise-wide changes and ensure that we hold Oracle Cerner accountable to make sure those changes happen—only then can we scale to large facilities.

As part of the reset, VA is making sure that our clinicians know we will support them. Through Dr. Evans and the EHRM leadership team, we’re starting to be able to address those proposed changes. As progress is made, I’m committed to keeping those open lines of communication, and making sure those five locations have the support that they need to be able to continue to execute and to take care of our Veterans, because that's the most important mission that we have.

3. **There has been a lot of discussion on the costs of the EHR modernization effort. One of the main drivers of these costs is new requirements being added by VA.**

a. **If confirmed, what mechanisms would you rely on to control costs and ensure we are prioritizing dollars for enterprise capabilities and not the customized needs of every VA site?**

I believe VA must be a responsible steward of taxpayer dollars. To ensure we are effectively managing requests for new requirements and not meeting the customized needs of every site, I am committed to continuing VA's efforts in establishing governance bodies and processes for clearer and more rapid decision-making. For example, one of the most impactful outputs of the Sprint was the establishment of VHA EHRM governance bodies and processes to ensure enterprise standardization and health system decision-making.

From a cost control perspective, I understand that VA notified Congress that the EHRM program will not be seeking the 25% funding withhold (totaling $439,750,000) of the VA EHRM budget line for FY 2023 due to the overall program reset. Another mechanism to cost controls is the re-negotiated Oracle Cerner contract, which now includes stronger performance metrics and expectations, as well as larger monetary credits to VA if Oracle Cerner doesn't meet expectations. For example, if these new terms had been in place since the start of the contract, VA would have received approximately a 30-fold increase in credits for the system outages. And outage-free time is only one of the 28 performance metrics that are now built into the contract, so Oracle Cerner is heavily incentivized across the board to improve performance for Veterans and clinicians.

As part of the reset, I am committed to working with Congress on resource requirements for the agency's EHR Modernization efforts. When the reset period concludes, I would ensure that VA will update its EHR deployment schedule and program life cycle cost estimate and will provide an updated version to Congress once completed.

4. **Senator Grassley' office has received multiple legally protected whistleblower disclosures related to the VA's Integrated Enterprise Workflow Solution (VIEWS) system, which VA uses to manage and track its correspondence. The VIEWS system is under your authority as VA's Chief of Staff.[1] Whistleblowers have provided records asserting that the system is used to store extremely sensitive information, including correspondence from members of Congress, confidential whistleblower information, personal identifiable information (PII), and protected veterans' medical**

[1] Liberty IT Solutions, summary, VA integrated Enterprise Workflow Solution (VIEWS) Salesforce Development (last accessed May 31, 2023) (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), https://appexchange.salesforce.com/partners/servlet/servlet.FileDownload?file=00P3A00000iHXXiUAO.

records and health information (PHI). The records illustrate that sensitive information is not being marked as sensitive and segregated from less sensitive documents in the system.[2]

The information is accessible to thousands of VA employees with access to VIEWS. These VIEWS users, according to whistleblowers, do not have to enter login credentials each time they access the system, and instead log in to the system once, with no dual factor authentication or other typical security measures to secure their access.

Emails show that your Deputy Chief of Staff, Maureen Elias, was made aware of serious security flaws in the VIEWS system in July 2022 by a certified fraud examiner.[3] **Moreover, the Office of Special Counsel (OSC) was apprised of a major security vulnerability and on August 2, 2022, OSC determined that there was a "substantial likelihood of wrongdoing" with respect to potential violation of federal privacy laws related to VIEWS.**[4] **OSC ordered Secretary McDonough to launch an investigation and complete it within 60 days; however, it has yet to be completed.**[5] **Based upon information from whistleblowers, the VIEWS system still has these serious security vulnerabilities, nearly a year after you were notified.**[6]

a. **Does VIEWS properly secure sensitive correspondence, PII, PHI, and whistleblower information? If not, why not? If so, please explain**.

I take the privacy of the Veterans, families, caregivers, and survivors that we serve extremely seriously and will continue to do everything in my power to protect it. I also take all whistleblower allegations seriously and will work with VA's Office of Information and Technology (OIT) to take whatever steps are necessary to protect sensitive information, including developing dual factor authentication for VIEWS.

The Veterans Affairs Integrated Enterprise Workflow Solution (VIEWS) is a system implemented in 2018 to replace older processes and tools. It is used to manage various tasks, documents, and reports within the VA; however, it does not handle medical records, claims, benefits, or financial actions. Around 1,900 VA employees have access to VIEWS, which is a tiny fraction—less than half of one percent (0.05%)—of department employees.

[2] Records, including screenshots of the system, are on file with Committee staff.

[3] 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.

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

[5] According to OSC, they will apprise Mr. Rizzo when the report is complete, and they have yet to do so.

[6] Statement by Peter Rizzo, *supra* n. 4; screenshots of recent sensitive information tagged not sensitive are on file with Committee staff.

VIEWS runs on a secure platform called Salesforce Government Cloud Plus, which has been approved by more than 40 federal agencies. The system is regularly checked by VA's Privacy Officer and Information System Security Officer to ensure the safety of sensitive information. These officials have issued annual Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) reports affirming that VIEWS is appropriate for sensitive information, including most recently in Fall 2022. VIEWS has been FedRAMP certified with an authorization date of November 2, 2020.

The VIEWS system has controls in place to protect personal and sensitive data, with only specific designated team members permitted to access sensitive cases. Any other user lacking permission who attempts to access a sensitive case cannot see the case information or attachments relating to the sensitive matter. All employees using VIEWS must complete mandatory training, and system access is logged. Audits also are done to make sure information on the VIEWS system is accessed appropriately. VA and Salesforce, the platform in which VIEWS is run, follow strict security and privacy guidelines in accordance with national standards and VA policies.

b. When did you first become aware that sensitive correspondence, PII, PHI, and whistleblower information stored on the VIEWS system was not being marked as sensitive and therefore available to all VA employees with access to VIEWS? Upon being made aware, when and what steps did you take to properly secure access?

I first became aware that there were concerns relating to the treatment of sensitive information on the VIEWS systems shortly after certain VA employees approached my Deputy Chief of Staff in July 2022. Upon receiving that information, I met with representatives of the Executive Secretariat, which is the VA unit responsible for overseeing use of the VIEWS system. As a result, VA has undertaken a number of measures to further strengthen protections of private and sensitive information in VIEWS, including security enhancements, limiting access, and improved training. I have been informed that, in particular, VA has done the following:

i. In October 2022, the Managing Cases in VIEWS Case and Correspondence Management training course, one of the three video training courses required to obtain a VIEWS account, was updated to include a portion that addresses sensitive information. The video reminds users to mark a case sensitive if PHI, PII or Sensitive Personal Information (SPI) is recorded in the case. The training informs that PHI is health information in any form, including physical records, electronic records or spoken information. Several examples of PHI, PII and SPI are also presented within the training. Users also have the option to download a handout related to this training for their reference and future use.

ii. In November 2022, there were several system enhancements and updates related to application privacy and security initiatives. Specifically, this release included changes to the security features dealing with access and visibility of sensitive cases and case tasks, making Case Sensitivity a required field when creating a case and only allowing Case Owners to change ownership on sensitive cases.

This release also included revisions to the banner messages displayed for sensitive cases and case tasks, the case sensitivity help text and defect fixes to these messages identified in lower testing environments. Additionally, this release included updates to Congressional Letters case types to include defaulting to sensitive when a case is created and revisions to the banner message displayed when case sensitivity is set to Pending Review. Finally, this release included sustainment remediation fixes so that VIEWS processes remain current and up-to-date to meet ongoing Salesforce development standards.

iii. On December 7, 2022, VIEWS Office Coordinator (VOC) were informed that each Program Office and Administration could have no more than three VA employees identified as a VOC; and reminded of the importance of proper handling sensitive cases/information in VIEWS. VOCs are responsible for sharing relevant information they receive with their VIEWS users. This is related to a March 2022 requirement for VIEWS Office Coordinators to ensure that their roster of VIEWS account users is accurate. A quarterly review of each VOC’s user roster is conducted, and accounts of users who have either moved to a different office or left the VA altogether are removed. Twice a year these reports must also be reviewed and verified by all Administrations’ and Staff Offices’ Chiefs of Staff.

VOCs also were reminded that accounts with no activity after 90 days would be deactivated, and they were also provided a new additional step for reactivating an account after it is deactivated due to inactivity. VOCs are required to obtain approval from the Program Office’s or Administration’s Chief of Staff before submitting a request to reactivate a recently deactivated account.

iv. To further enhance the security of VIEWS and access, the Department is implementing the following in June-July 2023:

- Accounts will be deactivated after 45 days of inactivity versus 90 days and will still require Program Office’s or Administration’s Chief of Staff approval for reactivation (effective June 26, 2023), and
- Potential new users requesting a VIEWS account must meet three role-based criteria and their first-line supervisor must approve the new account request (effective July 10, 2023).

v. The Department also has been exploring the feasibility of adding two-step authentication when logging into VIEWS.

Also, on August 2, 2022, VA received a letter from the Office of Special Counsel referring for investigation the allegations raised regarding VIEWS. The OSC letter also was provided to the Office of Inspector General which, after making initial inquiries, declined to open an investigation. VA also briefed House Veterans Affairs Committee staff on the VIEWS systems and issues concerning its protections for private and sensitive information. Finally, VA designated its Office of Information and Technology (OIT) to investigate the allegations raised by OSC. VA currently expects this OIT investigative report relating to VIEWS to be submitted to OSC by August 1, 2023. I look forward to receiving OIT's recommendations and will ensure their recommended changes are promptly implemented.

c. **When you became aware of the apparently major security vulnerabilities in VIEWS, did you request a forensic investigation or audit be conducted to determine whether the information may have been misused? If so, when did you request it, and what were the results? If not, why not?**

Within weeks of my first being informed of the concerns raised about VIEWS, VA received the OSC letter which addressed the same issues. In accordance with that letter, VA designated OIT to conduct an investigation into the allegations. I have had no responsibility for, or role in, overseeing the OIT investigation of these VIEWS issues. In light of the ongoing OIT investigation, I did not request a forensic investigation or audit.

i. Are you aware of any specific incidents of whistleblower retaliation, doxing, identity fraud, or any other negative consequence to individuals that may be linked to information in VIEWS being accessed inappropriately? If so, what steps did you take in response to this knowledge?

No.

ii. When were you notified of the July 2022 complaint about the security vulnerabilities in the VIEWS system?

See response to Question 4b above.

iii. In detail, what steps did you take after learning of this complaint to investigate or remedy the security flaws identified? When were these steps taken?

See response to Question 4b above.

iv. Are the security flaws identified in July 2022 still present in the VIEWS system? If so, why have they not been fixed or use of the VIEWS system for storage of sensitive information suspended until they are?

I defer to the results of the OIT investigation, conducted at OSC request, regarding whether there are security flaws in the VIEWS system that have not been remedied.

v. What is the status of the investigation of the VIEWS system ordered by OSC?

I have been told that OIT expects to submit the results of its investigation into the VIEWS allegations to OSC by August 1, 2023.

vi. Have you been interviewed or in any way consulted in this investigation?

No.

vii. Why has the VA requested extensions from OSC to complete the VIEWS investigation, and what interim steps have been taken to remove or secure sensitive data on the VIEWS system?

I have had no responsibility for, or role in, overseeing the OIT investigation of these VIEWS issues and am not aware of why VA has requested extensions from OSC to complete the VIEWS investigation.

viii. Does VA have a data governance strategy in place? If not, why not?

I have been informed that VA developed an Enterprise Data Strategy in January 2021. The Office of Enterprise Integration (OEI), in coordination with the VA's Data Governance Council (DGC), published a Data Management Directive, which establishes VA policy and defines roles and responsibilities for data governance and management throughout the Department. The Directive mandates that all data will be inventoried, cataloged, and systematically available for responsible sharing consistent with VA's I CARE core values, law and policy, VA Data Guiding Principles, and VA's Ethical Principles for Access to and Use of Veteran Data. The Directive emphasizes data protection, privacy and confidentiality; aligns with the appropriate standards and architectures; and ensures visibility of its quality and permitted uses. The Enterprise Data Strategy builds on the Directive and sets the vision for VA to leverage data as a strategic asset. Managing VA's data as a strategic asset across its lifecycle, via the framework set in this strategy, is the necessary precondition to further strengthen VA's delivery of services and benefits to the Nation's Veterans, their families, caregivers and survivors.

VA also has established a Data Governance Council (DGC) under the VA Operations Board (VAOB) to ensure use of agency data as a strategic asset and supports the Secretary's strategic goals to improve the lives of Veterans, caregivers, and their families. DGC is VA's primary organization charged with directing the process of setting and enforcing priorities for managing and using data as a strategic asset.

ix. **If these serious security flaws have been allowed to exist unremedied in the system under your authority for so long, why should the Senate confirm you to a position where you will be in charge of the modernization of veterans' electronic health records (EHR), which contain sensitive PII and PHI?**

I take the privacy of the Veterans, families, caregivers, and survivors that we serve extremely seriously and will continue to do everything in my power to protect it. I was informed that the VIEWS system was thoroughly analyzed for privacy and security concerns before it was implemented in 2018. It has been subject to annual reviews and repeatedly been certified by the VA's Privacy Officer and Information System Security Officer. Following the concerns about the VIEWS system being brought to my attention, VA has taken substantial steps to improve and enhance the security and privacy protections of the VIEWS system. And if confirmed as Deputy Secretary, I commit to carefully reviewing the OIT and OSC review and taking whatever steps are necessary to ensure that the confidentiality of PHI, PII, whistleblower, and other sensitive information is properly protected.

5. **A report issued by VA's Office of Inspector General (OIG) in 2021 calls into question the appropriateness of storing sensitive information on the Salesforce system, which is the platform on which VIEWS is hosted.[7] Unless VA has taken appropriate technical steps to assure the Salesforce platform used for VIEWS complies with official industry and government standards for high-risk data, this may mean that even if appropriate sensitivity tags are applied within VIEWS, the system still would not be secure enough to store PHI, PII, and other sensitive data.**

   a. **Are you aware of this OIG report and its analysis of the relative security of the Salesforce platform? When did you become aware?**

   I was aware of this OIG report at approximately the time that it was issued in 2021.

   b. With respect to the OIG's findings in its 2021 report, has the VA proactively applied those findings in that report to fix security shortcomings in VIEWS?

   VA has satisfactorily addressed all of the OIG's recommendations in the 2021 report, with the OIG having closed all of these recommendations. It also is my understanding from OIT personnel that none of the OIG report's findings indicate any security shortcomings in VIEWS.

[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.

c. **Has VA taken appropriate steps to make sure the Salesforce application used for VIEWS has sufficient security to store PII, PHI, whistleblower information, and other sensitive correspondence? If so, what steps were taken, and when were they taken? If not, why not?**

I am informed that, as noted above, Salesforce is a FedRAMP High Baseline account which supports the government's most sensitive, unclassified data in cloud computing environments, including data that involves the protection of life and finances. FedRAMP is a United States federal government-wide compliance program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. VIEWS has an Authority To Operate (ATO) at a Minor Application Moderate with Privacy based on Security and NIST standards. In light of the VIEWS ATO, there was no requirement to remediate any security shortcomings since ATO is a clearance that VA gives to business partners who meet strident VA standards to develop systems, products, and processes for VA use. VA ATO reflects that all applicable security standards are met and that sensitive information is protected.

d. **Does the VIEWS system meet industry and federal standards for the storage of PII, PHI, and other sensitive data, including standards set by the National Institute of Standards and Technology for storage of PII and PHI? If not, why not?**

I am informed by VA OIT that the VIEWS system is fully compliant with industry and federal standards, including VA HDBK 6500, NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. See also response to Question 4a above.

e. **If VIEWS does not comply with these standards, in detail, what concrete steps have you or other relevant VA officials ordered to bring it into compliance?**

VIEWS complies with these standards.