Sen. Moran
Senate Veterans' Affairs Committee
Nomination of Tanya Bradsher to be Deputy Secretary
June 15, 2023

Questions for Tanya Bradsher
Ms. Bradsher, I appreciated your timely responses to the Questions for the Record submitted by the Members of the Senate Veterans' Affairs Committee following the May 31 hearing to consider your nomination to be the Department of Veterans Affairs (VA) next Deputy Secretary. I have additional questions regarding the VA's Integrated Enterprise Workflow Solution (VIEWS) system.

1. **You mentioned first becoming aware that there were concerns relating to the treatment of sensitive information on the VIEWS systems shortly after certain VA employees approached your Deputy Chief of Staff in July 2022.**

   In an email exchange with your Deputy Chief of Staff in July 2022, a VA employee specifically stated, "My safety is at risk. Since this [VIEWS issue] has been discovered I have been extremely stressed and am not sleeping well. My bank account was compromised approximately a year ago and money was stolen from me . . . I am scared to death knowing that everything I reported – 76 case files worth, is on full display for everyone in VIEWS to see . . ." In the same email chain, your Deputy Chief of Staff fully acknowledged another VA employee's note that included "anyone with VIEWS access can find this information on _____, leaving the door open to her continued harassment and doxing," and that "we suspect this has already happened to _____."

   However, you responded to committee questions stating that you are not aware of any specific incident of negative consequence to individuals that may be linked to information in VIEWS being accessed inappropriately. Were you not made aware of the detail noted above? If not, how were you made aware of concerns relating to the treatment of sensitive information on the VIEWS system after VA employees approached your Deputy Chief of Staff in July 2022?

   I first became aware that there were concerns about the VIEWS systems shortly after certain VA employees approached the Deputy Chief of Staff in July 2022. However, I was not informed at that time or in subsequent conversations about any issues with specific individuals' information, nor was I ever told that any individual's private or sensitive information had been improperly accessed on VIEWS.

2. **After receiving a letter from the Office of Special Counsel on August 2, 2022, referring for investigation the allegations raised regarding VIEWS, on what date did the Office of Inspector General inform the VA of its decision to decline to open an investigation?**

   VA was informed that the OIG declined to take the case on September 8, 2022.

3. **After receiving a letter from the Office of Special Counsel on August 2, 2022, referring for investigation the allegations raised regarding VIEWS, on what date did the VA designate its Office of Information and Technology (OIT) to investigate the allegations? Who made this decision? To what extent were you involved in the decision-making process? Do you know why the decision was made to delegate the investigation to OIT rather than to your office, which bears ultimate responsibility for VIEWS?**

   The investigation requested by OSC was assigned to OIT on September 9, 2022. This decision was based on the nature of the allegations, which concerned whether the VIEWS system comported with federal law and agency directives relating to the protection of private and sensitive information. OIT had expertise with the technology as well as the relevant laws and policies. OIT also had experience conducting investigations on behalf of OSC in the past. Accordingly, VA believed that OIT was best situated to conduct a review of the VIEWS system, and so it assigned this investigation to OIT.

4. **The same employees who raised concerns with your Deputy Chief of Staff detailed above, report that there has been no follow up from your office, nearly a year later, and that the information they requested to be protected remains openly accessible to nearly 2,000 VIEWS users.**

   Shortly after the Deputy Chief of Staff was contacted, we received a letter from the Office of Special Counsel referring for investigation the allegations raised regarding VIEWS. Following the assignment of this investigation to OIT, I expected the OIT to interview the employees who raised concerns and to keep those employees apprised, as appropriate, regarding the investigation. Also, if any sensitive information of these employees was not being properly protected by the VIEWS system, I would expect that to be immediately addressed and promptly remedied as part the OIT investigation.

   a. Did you direct anyone to follow up with the concerned employees to learn more about their concerns?

      i. If so, who did you assign and when? Please provide documentation.

      ii. If not, why not?

   My Deputy Chief of Staff had several conversations with the employees who raised issues about VIEWS in Summer 2022, in which she learned more about their allegations. However, within weeks, the allegations were assigned to OIT for investigation, and it was our understanding that the OIT investigators would interview these employees and address their concerns.

   b. Did you direct anyone to make sure that those concerns were addressed as soon as possible?

      i. If so, who did you assign and when? Please provide documentation.

ii. If not, why not?

As I have previously explained, soon after allegations were raised with the Deputy Chief of Staff, I met with representatives of the Executive Secretariat, which is the VA unit responsible for overseeing use of the VIEWS system. We discussed the importance of ensuring that the VIEWS system protected private and sensitive information, and I directed Executive Secretariat to work to further strengthen such protections. As a result, VA has undertaken a number of measures over the past year to improve the privacy and security of VIEWS, including security enhancements, limiting access, and improved training.

c. Did you direct anyone to follow up with the concerned employees after addressing their concerns?

i. If so, who did you assign and when? Please provide documentation.

ii. If not, why not?

As discussed in response to question 4 above, following the assignment of the investigation of the employees' allegations to OIT, I deferred to that investigation and expected the OIT investigators to be in regular contact with those employees who had raised allegations.

d. Did you follow up with anyone assigned with these responsibilities?

i. If so, who did you follow up with and when? Please provide documentation.

I have had no responsibility for, or role in, overseeing the OIT investigation of these VIEWS issues and have had no contact with the OIT investigators.

e. What actions will you now take to follow-up with the employees referenced?

Again, it would be my expectation that the employees who raised the allegations – some of whom have left VA – have been in regular contact with the OIT investigators and have been kept apprised of the investigation of their allegations, as appropriate. I would note that since the OIT was designated to investigate these allegations, these employees have not reached out to my office with questions or concerns. However, when the OIT investigation is completed, I anticipate OSC and/or VA will contact these employees to inform them of the outcome.

f. What actions will you take to ensure that no other employee who raises serious concerns with your office fails to receive an appropriate response?

I greatly value and appreciate when employees bring specific concerns forward and take all of their allegations seriously. As was done in this case, I will help ensure that their

allegations are fairly and thoroughly investigated. I also will ensure that employees who report concerns are not subject to any retaliation or adverse consequences for their having raised concerns.

5. **After you first became aware that there were concerns relating to the treatment of sensitive information on the VIEWS systems, you stated that you met with representatives of the Executive Secretariat, "the VA unit responsible for overseeing use of the VIEWS system." You note that "as a result [of that meeting], VA has undertaken a number of measures to further strengthen protections of private and sensitive information in VIEWS, including security enhancements, limiting access, and improving training." You also noted that you did not request a forensic audit because VA, "within weeks of my first being informed of the concerns raised about VIEWS," received an OSC letter ordering VA to investigate.**

   a. **When did you meet with the Executive Secretariat about this issue? Did you request the meeting or was it a regularly scheduled meeting? If you requested it, when did you do so?**

      I first met with representatives of the Executive Secretariat about this VIEWS issue in mid-July 2022. I regularly meet on a weekly basis with the Executive Secretariat to discuss a host of issues. Over the past year, Executive Secretariat has periodically informed me during these meetings about the steps it has been taking to further strengthen the protection of sensitive information in the VIEWS system.

   b. **Was the sole topic of the meeting the VIEWS system data security issues identified by the employee outreach to your Deputy Chief of Staff?**

      I do not recall.

   c. **What specific information did you share? Did you specifically request that the Executive Secretariat take measures to further strengthen the protection of private and sensitive information in VIEWS in this meeting? Why or why not?**

      While I do not recall the specifics of this initial meeting, over the past year I have discussed and supported the Executive Secretariat in taking various measures to further strengthen protections of private and sensitive information in VIEWS. As noted in my previous responses, a number of such improvements have been implemented over the past year. See Response to Senator Blackburn's Question 4a. VA also briefed House Veterans Affairs Committee staff on September 8, 2022 on the VIEWS system and how it protects private and sensitive information.

   d. **How do you distinguish between the "authority" you have over the VIEWS system and the "operation[al]" management that the Executive Secretariat performs?**

      As Chief of Staff, I am ultimately responsible for the VIEWS system. The Executive Secretariat uses the VIEWS system on a daily basis and is the VA unit responsible for overseeing the business requirements of the VIEWS system

e. Why were the employees who approached your Deputy Chief of Staff to express serious concerns with the VIEWS system not informed of the action you took to meet with the Executive Secretariat and the Executive Secretariat's work to implement additional protective measures?

Shortly after the allegations regarding the VIEWS system were brought to my attention, on August 2, 2022, VA received a letter from the Office of Special Counsel referring these allegations for investigation. As discussed above, following the assignment of the investigation of the allegations to OIT, I deferred to that investigation and expected the OIT investigators to be in regular contact with those employees who had raised the allegations.

f. You cited the investigation ordered by OSC as a reason you did not request an audit, but can you explain why that would have prevented you from asking for that audit, since the VA was in charge of the investigation and presumably could have set its parameters?

Because OIT was investigating the matter, I did not believe an additional audit was necessary. I commit to carefully review the OIT report and take whatever steps are necessary to ensure that the confidentiality of sensitive information in VIEWS is properly protected.

6. In your response to committee questions about sensitive information unsecured in VIEWS, you said that VIEWS, "does not handle medical records, claims, benefits, or financial actions." You also noted that, "the VIEWS system has controls in place to protect personal and sensitive data, with only specific designated team members permitted to access sensitive cases… 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."

a. How are these logs used, and how are these audits conducted? What parameters are applied? How much of the VIEWS system is audited, and at what frequency?

Logs are generated by DTC using their Splunk data logging tool. Major user activities are logged, such as login date and time, etc. Information is displayed on self-service dashboards for managers to review and monitor. The VIEWS system is audited in connection with receiving an Authority To Operate (ATO) at a Minor Application Moderate with Privacy based on Security and NIST standards. The VIEWS system also 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.

b. Has the VA audited the specific whistleblower and PII information brought to your office's attention in July 2022 for potential misuse?

Not that I am aware of. However, I do not know what audits or other reviews have been performed by the OIT as part of its ongoing investigation.

c. Have the VA audits you referenced detected any instances of unauthorized access by VA employees or instances of misuse of that data? If so, describe the number of instances and nature of those findings.

Not that I am aware of. However, I do not know what audits or other reviews have been performed by the OIT as part of its investigation and, if so, the findings of such audits. 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.

d. When a case is marked sensitive, are unauthorized viewers able to view anything about that case, even if they aren't able to view the attachment or body of the text? For example, are they able to view the title of the email or attachments?

No. A user who is not a member of the specific Case Team will be able to see only the Case ID number and a banner message indicating that they should contact the Case Owner for more information.

e. How often do VA employees undergo mandatory training for the VIEWS system? Does such training include an assessment of understanding? Is there a mechanism within the VIEWS system to track compliance?

Before being provided log-in access to the VIEWS system, an employee must complete 3 training courses by accessing the Information Technology Workforce Development (ITWD) training platform, including "Introduction to VIEWS Case and Correspondence Management (CCM)" and "Managing Cases in VIEWS Case and Correspondence Management." The training provides explanations regarding case sensitivity and explanations of PII/PHI. Several of these Web-based training courses include "knowledge checks," which are intended to help the student assess their understanding of the content.

In addition, all employees are required to take annual privacy training which focuses on protecting PII and PHI information. This training provides information security and privacy training important for all VA staff who use information systems or handle sensitive information. It identifies the types of information that must be carefully handled to protect privacy; describes the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explains how to report incidents. It also includes an assessment of the individual's understanding of what was learned during the course of the training.

Training completion reports are available from ITWD. Employees who request access to VIEWS CCM for the first time are required to submit evidence of having completed the required training courses before their user accounts are provisioned.

f. Isn't it true that sensitive medical, claims, benefits or other information would be in the VIEWS system if it was part of VA correspondence tracked in the system?

Yes.

7. **In your response to committee questions, you noted that in June-July 2023 the Department intends to deactivate VIEWS user accounts after 45 days of inactivity rather than 90, and require new users to meet three role-based criteria and receive first-line supervisor approval. How many current VIEWS system users do you anticipate there will be following the implementation of these measures?**

   I am told that we will not know the extent of the reduction of users until approximately 30-60 days after the change takes effect.

8. **In your response to committee questions, you note that VA is "exploring the feasibility of adding two-step authentication when logging into VIEWS." How is VA exploring such feasibility and when do you expect a decision to be made about the feasibility of adding two-step authentication in order to access the VIEWS system?**

   VIEWS is accessible only on VA-owned and managed laptop and desktop PCs. Employees accessing VA-owned desktop computers are required to have in their possession a validated, VA-owned Personal Identification Card (PIV) and Personal Identity Number (PIN); without such physical credentials and information the desktop computer cannot be used. Consequently, VIEWS, via the Microsoft Edge Web browser, already inherits two-factor SSL security authorization from the computer.

   However, to further enhance privacy and provide another layer of security, OIT has requested the DTC (Digital Transformation Center, the office responsible for running the Salesforce platform) to conduct a feasibility study for adding application-level two-factor authentication. OIT has requested that VIEWS CCM users be presented with a security warning banner message upon logging into the system, which they must acknowledge with a button click, and then they will be prompted to select their PIV credential and enter their PIN. All access attempts, whether failed or successful, will be logged with typical date and timestamps, computer name, and other information to be determined based on recommendations and security best practices. VA expects a preliminary response from DTC within one month. If this feasibility study confirms that the capability can be implemented on the Salesforce platform, then a full timeline of events will be established.

9. Is it your understanding or belief that your ability to act in response to employee concerns about the VIEWS system is in any way hampered by the OSC or the ongoing OIT investigation? If so, what is that understanding or belief based on?

I do not believe the OIT investigation prevents us from taking steps to address issues relating to the VIEWS system's protection of sensitive information. For that reason, over the past year 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. See Response to Senator Blackburn's Question 4a. I commit to carefully review the OIT report and take whatever steps are necessary to ensure that the confidentiality of sensitive information on VIEWS is properly protected.

10. What accountability do you believe that you bear for the ongoing concerns regarding the VIEWS system?

I am responsible and accountable for the VIEWS system. As I previously noted, only a tiny fraction—less than half of one percent (0.05%)—of department employees have access to VIEWS. 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.

Since allegations regarding VIEWS were raised last summer, 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. VA also has designated OIT to conduct an investigation of the allegations regarding VIEWS. OIT's report on the results of its investigation is expected to be submitted to OSC by August 1, 2023. I commit to carefully review the OIT report and take whatever steps are necessary to ensure that the confidentiality of sensitive information on VIEWS is properly protected.

In regard to my question about employee accountability actions taken by the Department, thank you for the data chart displaying total adverse actions in each year from fiscal year 2016 to fiscal year 2022. I remain interested in reviewing whether or not

use of the authority had the intended impact of expediting removal processes from those occurring before passage of the Department of Veterans Affairs Accountability and Whistleblower Protection Act of 2017.

11. Please provide the average time, from beginning of disciplinary process to completion, that it took for VA to administer these adverse actions in each year from fiscal year 2016 to fiscal year 2022.

I am told that VA established a Department-wide human resources (HR) information technology system to collect, monitor and report data related to employee relations matters in July 2020. Prior to this date, there was no enterprise-wide system of records for employee relations data and reporting. As a result, we cannot determine whether or not use of the authority had any impact on the time of the removal processes during fiscal year 2016 to fiscal year 2022. Based on information currently in the system for fiscal years 2020, 2021, and 2022, we can report that the average time to process an adverse action starting with receipt of an evidence file and ending with issuance of a decision was between 56 and 69 days during that time period.

In regard to my question about the timeliness of VA's responsiveness to Congressional inquiries, I appreciate that, if confirmed, you would hold the Deputies of each of the administrations and departments accountable for timely testimony, requests for information, letters and general inquiries from Congress.

12. What exact steps would you take if confirmed as Deputy Secretary to improve the timeliness of VA's communications with Congressional stakeholders and how will you ensure accountability for maintaining timeliness and transparency?

If confirmed as Deputy Secretary, it will be a priority of mine to hold VA accountable to maintaining timely and transparent communications with this Committee and our Congressional stakeholders. The first step along this path of continuous improvement is to ensure collaboration between members, staff, and VA leadership. Lessons learned as a congressional staffer about the importance of a respectful and responsive relationship with Committees would inform my approach to proactively sharing information. I have observed that a strong and productive exchange between VA and Congress is reflective of the amount of ongoing collaboration and continuous outreach to strengthen the relationship. My goal will be to keep in regular touch with this Committee and members of Congress so that they can continue their work to help Veterans, and I will continuously monitor VA's performance and identify any trouble spots.

Second, I would convene a regularly occurring meeting with the Deputies across VA's administrations where we can discuss the status of existing requests from Congress and address any causes for delay. This will not only give us greater insight into where responses are getting stuck but will also provide an opportunity to increase cross-talk and communication. Without the support of the program and staff offices, VA cannot provide

Congress with accurate, reliable information and data on VA's programs, updates on execution of its priorities or technical assistance on legislation

Third, I would work across administrations to apply human-centered design approaches to improve and streamline the processes. For example, not all inquiries require the same amount of effort. There are yes-and-no queries that should have quick turnaround, whereas pulling significant data and information could take longer. While one-size-fits-all benchmarks might not make sense, it does make sense that Congress gets useful information it needs to do its job, within a reasonable timeframe.

Lastly, I will work with the Office of Congressional and Legislative Affairs and the Office of Enterprise Integration to continuously monitor VA's performance and identify any trouble spots.

13. Do you acknowledge the role of Congress in the oversight of federal agencies as essential to the legislative powers vested in Congress by Article I of the Constitution?

Yes. It is my understanding that Supreme Court has stated: "the power of inquiry–with process to enforce it—is an essential and appropriate auxiliary to the legislative function" *McGrain v. Daugherty*, 273 U.S. 135, 174 (1927). As a former congressional staffer, I fully appreciate the importance of Congress's oversight role which helps make VA better in fulfilling its mission of providing world-class care and benefits to Veterans.

14. Do you recognize that Congress is exempt from regulations, laws, and policies that would otherwise prevent the disclosure of private information about veteran patients?

It is my understanding that while Congress has exempted itself from some regulations, laws, and policies that would otherwise prevent the disclosure of private information about Veteran patients, Congress does not enjoy a blanket exemption and any exemptions may not be absolute and may depend on the particular facts and circumstances. Nevertheless, I will seek to provide information in response to Congressional requests to the fullest extent consistent with executive branch policies and practices and the law.

15. What role, if any, do you think the Department should have in determining the validity of Congressional oversight requests?

Upon receipt of a properly authorized oversight request, the Executive Branch's longstanding policy has been to engage in the accommodation process by supplying the requested information to the fullest extent consistent with the constitutional and statutory obligations of the Executive Branch.

16. **Please provide the number of Veterans Care Agreements that have been entered into to-date pertaining to the interim final rule on reproductive health.**

I have not been involved in developing or implementing the Reproductive Health Services IFR (87 Federal Register 55287). I will refer your question to the Veterans Health Administration to coordinate with the Office of Congressional and Legislative Affairs in providing a response.

17. **Please provide, in full, all the training materials, recordings, documents, and modules provided to VA employees by the Department pertaining to the interim final rule on reproductive health.**

I have not been involved in developing or implementing the Reproductive Health Services IFR (87 Federal Register 55287). I will refer your question to the Veterans Health Administration to coordinate with the Office of Congressional and Legislative Affairs in providing a response.

18. **Please provide, in full, a complete list of the relevant medical diagnoses that have resulted in referrals for abortion under the health exception included in the interim final rule on reproductive health.**

I have not been involved in developing or implementing the Reproductive Health Services IFR (87 Federal Register 55287). I will refer your question to the Veterans Health Administration to coordinate with the Office of Congressional and Legislative Affairs in providing a response.