

United States Senate

WASHINGTON, DC 20510

September 16, 2020

The Honorable Robert Wilkie
Secretary of Veterans Affairs
810 Vermont Ave, NW
Washington, DC 20420

Dear Secretary Wilkie,

We write today to express our serious concerns with the Department of Veterans Affairs' (VA) continued inability to protect the personal data of veterans and those medical providers in the community who partner with VA to provide veterans timely access to health care. Veterans who rely on VA for health care and providers who do business with VA need assurance that the Department is capable of safeguarding their personal and financial data. Anything less is completely unacceptable.

On September 14, 2020, VA publicly announced that approximately 46,000 veterans were impacted by a data breach involving their personal information. In addition, while not mentioned in VA's press release, VA officials informed the Senate and House Committees on Veterans' Affairs that approximately 17,000 VA community care providers who utilize Veterans Care Agreements (VCAs) to provide health care to veterans were also impacted. Based on information currently available, it appears this cybersecurity incident was carried out by those able to find weaknesses in the way VA authenticates community care health care providers using VCAs and processes payments for their services. This cybersecurity incident means that Social Security numbers and potentially other personally identifiable information (PII) of veterans have been exposed as well as bank account information for thousands of community providers. We fully support the VA Office of Inspector General's (OIG) ongoing investigation into this matter.

This incident raises numerous concerns not just for this incident, but more broadly with how VA is approaching protecting the PII and other important data within its vast data systems and networks. This is not a new vulnerability for VA. Rather, it is a long-standing weakness of the Department as identified by independent reviews conducted by the VA OIG and the Government Accountability Office (GAO) for more than 10 years. The information provided to Congress on this incident raises countless questions and does not instill confidence that VA is adequately addressing the current incident or working to better safeguard private information in the future. As such, we request you provide us with answers to the following questions so that we may perform appropriate oversight of the Department's management of cybersecurity, risk management, and veteran data protection:

1. In the VA press release issued on September 14, 2020, VA directs veterans or their next-of-kin with questions to contact VA by e-mail or postal mail. Recognizing that some veterans do not use or have access to e-mail and that postal mail is experiencing challenges due to management decisions made by the Postmaster General, why is a Toll-Free phone number not provided?
2. Provide a state-level breakdown of the impacted 17,000 community providers.


3. What actions is VA taking to assure community providers working with VA that doing business with the VA is safe and that their financial data will be secure?
4. Did the Department discover the data breach on its own or was it first identified by the VA OIG?
5. In briefings with Committee staff, VA indicated that up to 85 different VA Financial Services Center (FSC) systems operated under one Authority to Operate (ATO), including the Customer Engagement Portal (CEP) where this data breach occurred.
 - a. Provide a list of the 84 other systems operating under this ATO.
 - b. For each of the 85 systems, please provide the purpose of each system, the number of users, the types of users (internal/external/veteran/non-veteran), monthly transaction volume, and other pertinent statistical data.
6. It appears the Department remains in a reactive posture, waiting for cybersecurity or business rule vulnerabilities to arise. What proactive assessment of systems for vulnerabilities in business rules does VA's OIT conduct regularly across the VA enterprise and with what frequency?
7. On August 7, 2020, VA issued a Request for Information (RFI) to solicit information from industry on cybersecurity audit services. The RFI includes a description of audit services tasks such as that "[t]he Contractor shall perform an overall cybersecurity audit assessment for all control families across all FSC major and minor systems under the Authority To Operate (ATO)... The Contractor shall provide a GAP analysis on which cybersecurity tools, processes, and controls the Government should employ and provide recommendations of methods to improve visibility as well as incident response time following VA best practices."
 - a. This RFI reflects a lack of very basic internal capabilities at the FSC, but also OIT and VA as a whole. Why has VA OIT not conducted an assessment like this for FSC already?
 - b. How many different VA organizations such as the Veterans Health Administration, Veterans Benefits Administration, and the National Cemetery Administration also need a similar review of their data systems and business rules for cybersecurity weaknesses?
 - c. Why is it the responsibility of these entities in VA to organize these reviews rather than have them led by VA's OIT?
 - d. Does VA currently have the ability to perform these services in-house?
8. What steps will VA take to conduct more oversight of its Franchise Fund Enterprise Centers, such as FSC, and the business rules, IT processes, and cybersecurity protocols they follow to identify additional potential vulnerabilities?
9. VA OIT officials who briefed the Committee on this current FSC incident appeared to indicate that the problems at the FSC were not VA OIT's responsibility and were solely a FSC concern. What steps will you take as Secretary to reinforce to your leadership team that in order for VA to succeed, VA OIT needs to 1) take responsibility for this incident and 2) take a more proactive approach to management of cybersecurity and business rule vetting and monitoring, which are a core function of VA OIT?

10. Are you concerned that VA's Office of Management (OM), responsible for "oversight of VA's internal control program and compliance with improper payments legislation as well as prevention of fraud, waste, and abuse" is the organization where this data breach occurred? What additional steps have you directed to ensure OM reviews all relevant protocols, organizational structures, and oversight mechanisms to ensure such an incident does not re-occur?
11. In July of 2019, the GAO issued a report entitled "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges." The report included dozens of recommendations for agencies, including four for VA focused on cybersecurity and enterprise risk management –topics directly applicable to the most recent data breach. Please provide a status of VA's efforts to close these critical recommendations, two of which GAO has labeled as Priority Recommendations. The recommendations are currently listed as open on GAO's website.
12. In June of 2019, GAO issued a report entitled "Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes." The report included several recommendations for agencies, including one for VA that GAO labeled as a Priority Recommendation. Please provide a status of VA's work to close this recommendation. The recommendation for VA is currently listed as open on GAO's website.


This most recent data breach is unacceptable. It also exposes the fact that VA has not taken the necessary steps to ensure oversight, accountability, and security of the vast financial, health, and other personal data it collects and processes to perform its critical services for America's veterans. Incidents such as these impact individual veteran's lives as well as those who partner with VA to provide services to them. It is imperative VA take aggressive and decisive action to address this current incident and lay out a strategy to prevent such problems from arising in the future.

We look forward to your prompt reply to these questions.


Sincerely,




Jon Tester
United States Senator



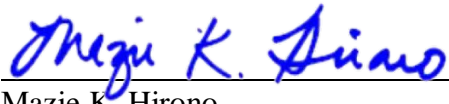
Patty Murray
United States Senator



Sherrod Brown
United States Senator



Richard Blumenthal
United States Senator



Mazie K. Hirono
United States Senator



Joe Manchin III
United States Senator



Kyrsten Sinema
United States Senator



Margaret Wood Hassan
United States Senator



Jeanne Shaheen
United States Senator