The Honorable Tim Walz  
Ranking Member  
Committee on Veterans’ Affairs  
U.S. House of Representatives  
Washington, DC 20515

Dear Congressman Walz:

In response to requests from several Members of Congress, I write to update you on the Office of Inspector General (OIG) review of recent allegations of “hacking” or other deceptive practices relating to former VA Chief of Staff Vivieca Wright Simpson’s VA email account.

Our administrative investigation report on VA Secretary and Delegation Travel to Europe referred to an altered June 2, 2017 email, which was forwarded from Ms. Wright Simpson’s VA email account to a VA ethics official and which provided the basis for VA’s payment of Secretary Shulkin’s wife’s airfare. Following release of the report on February 14, 2018, certain media reported, based on interviews with Secretary Shulkin, that Ms. Wright Simpson told him she did not alter the email and claimed to have been the victim of computer hacking.1 These reports implied that such hacking might explain how the June 2017 email sent from Ms. Wright Simpson’s VA email account was altered.

Given the relevance of these allegations to a central finding in our report,2 the OIG took them very seriously. After coordinating with attorneys from the Department of Justice’s Public Integrity Section, OIG investigators secured Ms. Wright Simpson’s VA-issued computers and mobile devices.3 The OIG also informed the Federal Bureau of Investigation that it had secured the relevant devices. For the reasons described below, however, the OIG does not believe that forensic analysis of Ms. Wright Simpson’s data is warranted at this time.

---

1 See, e.g., Arthur Allen, “VA audit: Aide expensed Shulkin’s wife’s European travel under false pretense,” Politico (Feb. 14, 2018), available at https://www.politico.com/story/2018/02/14/david-shulkin-europe-travel-347064 (“Wright Simpson denied having sent the email with altered information, and showed Shulkin evidence that her email had been hacked and that someone had been sending emails in her name, he said.”).

2 For more information on the alteration of the June 2, 2017 email, see Europe Travel Report at p. 5-6.

3 On February 16 and 20, 2018, OIG collected and secured Ms. Wright Simpson’s VA-issued computer equipment, including desktop and laptop computers, iPad, and iPhones. On February 23, 2018, OIG was given network access to secure Ms. Wright Simpson’s personal network and group drives.
In the nearly two weeks since the release of our report, the nature of the alleged compromise of Ms. Wright Simpson’s VA email account has become clearer. The OIG now believes that the allegations of “hacking” are limited to unrelated and relatively unsophisticated “spoofing” of Ms. Wright Simpson’s identity through messages sent from an external, non-VA email address.

The OIG has taken a number of steps that have led to this conclusion:

- We requested from VA copies of the evidence that Ms. Wright Simpson purportedly showed Secretary Shulkin on the morning of February 14, 2018. This consisted of a single chain of email messages marked “External” between a “comcast.net” email address using the display name “Vivieca Wright Simpson” and a VA finance employee. The emails had been sent that morning, February 14, 2018 purportedly seeking to obtain payment on a purchase order. Given the “External” markings and the comcast.net email domain, it is obvious from the face of the “Vivieca Wright Simpson” email that it did not originate from the VA email system.
- OIG investigators conferred with VA’s Information Technology (IT) staff, who were aware of no evidence that Ms. Wright Simpson’s actual VA email account was compromised during any period relevant to the Europe travel investigation or subsequently. The VA, in fact, issued a statement on February 16, 2018 that read, in part, “we have thus far found no credible or conclusive evidence of a compromise to our email system or a user’s account.”
- OIG counsel and I spoke with Secretary Shulkin and his counsel about this issue. Secretary Shulkin informed us that, in speaking with reporters about Ms. Wright Simpson’s allegations, he did not mean to imply that her VA email had been “hacked.” Secretary Shulkin said that he was not aware of any allegations relating to Ms. Wright Simpson’s email beyond the information she showed him on the morning of February 14—that is, the “comcast.net” email described above. (The OIG reached out to Ms. Wright Simpson through her counsel and requested the opportunity to speak with her about her allegations concerning spoofing or otherwise unauthorized email practices. Her counsel indicated that

---

4 Perhaps relatedly, on February 22, 2018, Scott Blackburn, the Executive-in-Charge of VA’s Office of Information Technology, issued an email to senior VA staff warning them of potential “whaling.” According to the memo, “We have recently been made aware of a phishing attempt targeting VA Leadership. Whaling, a specific form of phishing, attempts to trick senior leaders into divulging company information or private data by posing as a ‘legitimate’ source.”


6 See also Juana Summers, “Democratic Rep. Walz: Justice Department should investigate Shulkin’s hacking claim,” CNN (Feb. 15, 2018), available at https://www.cnn.com/2018/02/15/politics/shulkin-travel-email-justice-department/index.html (quoting Eric Nitz, one of Secretary Shulkin’s attorneys: “At this time, the Secretary knows of no evidence to suggest this incident relates to the events described in the IG’s report.”).
Ms. Wright Simpson was not available to meet with OIG investigators at this time. In an email to OIG counsel on February 24, 2018, her counsel did make clear that Ms. Wright Simpson “never asserted that her email was hacked.”

In an interview yesterday with USA Today, Secretary Shulkin confirmed that Ms. Wright Simpson’s VA email account had not been hacked: “I think what we know right now is that there was no compromise to the system…. I think—again I’m reaching beyond my expertise—but I think that there was no hacking, this was more what’s called spoofing, which is the impersonation of a person, but it’s not within the firewalls.” That statement is consistent with the evidence the OIG has seen.

We are also aware that VA IT staff have identified a type of phishing attack in which a VA employee is impersonated in an effort to convince another employee to reveal private information and potentially to obtain fraudulent payments. VA IT staff appear to be keeping VA employees informed and advised of actions they should take in response to such efforts. We will continue to work with the Department to monitor the alleged phishing/spoofing and stand ready to investigate all credible allegations of email and computer hacking or other violations at VA if additional evidence is developed.

If we identify any further information relevant to the allegations of “hacking” or other deceptive practices relating to Ms. Wright Simpson’s VA email account, we will update the Committee. Please let me know if you have any questions or need further information. I thank you for your consideration.

Sincerely,

MICHAEL J. MISSAL

---