United in Speaking Truth to Power

www.whistleblowersofamerica.org
601 Pennsylvania Ave, South Tower, Suite 900 Washington, DC 20004

Statement of

Ms. Jamie Fox

Before the House Committee on Veterans' Affairs

January 30, 2018

Chairman Roe and Ranking Member Walz;

Thank you for this opportunity today to speak out on behalf of veterans who are also VA employees. I am submitting this statement for the record in cooperation with Whistleblowers of America (WoA) because my situation is not unique. WoA has had several other veteran/VA employees make this same claim about having their private information weaponized. We are joining forces today in hope that this hearing will give voice to those of us who have had our privacy invaded after blowing the whistle on VA and to ask Congress, that as you consider legislative reform for the Veterans Benefits Administration (VBA), that you might also consider the need to further protect Claim or C-files and to allow veterans/employees to know who has accessed their personal information.

Let me begin by saying that I come from a long line of family members who have served in the military as far back as the Revolutionary War and who are currently serving in the military. I also served honorably for five years in the U.S. Navy. When I volunteered to serve in the military and civil service I did not volunteer to be subjugated to the unethical and illegal abuse of public office power. Since coming forward in 2008, as a witness for a former co-worker who was being harassed – in order to help her stop the harassment – I have been continuously harassed, punished, and retaliated against by the same people who protected the perpetrator. When I came forward that day in 2008, I thought there were laws that protected me. I utterly had no idea that such a simple gesture, like caring for the dignity of another human-being, would have such severe and far reaching negative consequences. What is and has been happening to me is unethical and illegal. Not only is it a breach of privacy, but it is also a breach of trust.

It is a disgrace when the very people who defend the rights of the American people do not have those same rights at the VA, particularly the right to have our private information protected from the people who we do not want to access our private information.

Many veterans wrongly believe their private information, which includes Personally Identifiable Information (PII) and Sensitive Personal Information (SPI) is protected by privacy laws, but at the VA this belief couldn't be further from the truth. Veterans' PII and SPI have more protection

in the civilian sector because there are very real and serious consequences for privacy violations, but there appears to be very little recourse for veterans whose privacy is violated by government officials at the VA.

According to Deven McGraw, Director of the Washington-based Health Privacy Project of the nonprofit center for Democracy and Technology, the VA remains one of the top Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy offenders. In April 2015, the Office of Special Counsel Director, Carolyn Lerner, testified in Congress that the prevalence of privacy violations at the VA has become an epidemic.

VA Office of Inspector General (OIG) released a report April 2016, in which the VBA had not integrated proper audit logs in their new veterans' claims processing computer system, called Veterans Benefits Management System (VBMS). In fact, VBA failed to establish satisfactory system requirements in VBMS that would ensure that accurate audit logs were created. Without accurate audit logs, Information Security Officers cannot effectively identify, report, and react to data security issues in VBMS. OIG discovered VBA cannot detect if an employee improperly accessed a claim and that VBMS was not compliant with audit log procedures and regulations. Further OIG reported that the security vulnerability occurred because the Office of Business Process Integration did not create system requirements in VBMS to assure audit logs could accurately pinpoint security violations. It assumed that the audit log functionality was already built into VBMS as it was for the legacy claims processing systems.

The VBA is required by several regulations (e.g., Federal Information Processing Standards Publication) to develop, sustain, and retain audit records to supervise, analyze, and report on inappropriate access of information systems. The VBA must also develop the capability to monitor the actions of individual users. VBA's own VA Handbook states that information systems are required to create detailed audit logs that can help recreate a data security incident.

As a veteran using the VA system, I recently discovered that I have absolutely no control over my private and protected information, and that VA managers have carte blanche to everything with impunity! Anyone who has access to VBMS with a few strokes of the keyboard can view over 30 years of information about me, from anywhere in the country, including from someone's living room.

No person, not even a government official, should have that much access to so much information about a person's past and present life history, especially VA employees who are known to be unscrupulous. No manager or former manager or co-worker should have access to so much information about their employees or co-workers, especially the people who were responsible for forcing my resignation and who I testified against for protecting the man who I witnessed harassing a co-worker. What I say to my doctor is no one else's business unless they absolutely have to view the information and were authorized to view the information. It is my right to see who has accessed my private information and it is my right to restrict who sees my information. It is incomprehensible to think the VBA failed to build in safeguards in its highly touted computer program, which was allegedly designed to make processing veterans' claims more efficient, but cannot restrict certain VBMS users from accessing specific claim files, except through an antiquated security system that was designed to control paper files. This antiquated

security system allowed and continues to allow people, like my former managers and co-workers, access to my protected information. It also allows managers and employees to snoop on current VA veteran employees and co-workers.

It's easier to conceptualize the outdated security control system as a pyramid, scaled 1 to 9, where 9 has the most restriction. The higher the sensitivity level, the fewer people who can view the C-file. The higher the sensitivity level the fewer people there are to help a veteran with their C-file. C-files that are classified at sensitivity level 8 and above cannot receive help from the public contact line and Veterans Service Organizations, even with simple tasks, like changing an address. The only way someone would not be able to view a C-file is if they did not have access to a particular sensitivity level. For example, if you are authorized to view sensitivity level 7 C-files then you could view C-files classified at sensitivity level 7 and below. Obviously, anyone who does not have a sensitivity level 7 clearance would not be able to view C-files classified at sensitivity level 7 and above. Managers can also authorize other managers or employees, depending on the sensitivity level, to work on a C-file classified at a higher sensitivity level for a limited time. So, as you can see, it really does not matter what sensitivity level a veteran's C-file is classified at, if VA managers can work around existing security features.

VA leadership is misrepresenting the capabilities of the Restricted Access Claim Center (RACC) at the St. Paul, Minnesota Regional Office (and other RACC locations) regarding the restrictions related to managers and co-workers from accessing a current or former employee's veteran C-file. I was told once my C-file obtained RACC protection that the Oakland VA Regional Office would no longer have access to my C-file. I disproved this claim when I scheduled an appointment to review my digital C-file at the Oakland VA Regional Office. I witness with my own eyes how Oakland managers can still access my private information. It appears the RACC only restricts people from making changes to a C-file.

I was also told by several VBA employees that if a co-worker or a manager accesses a veteran employee's C-file, an alarm gets set off - that some employees have referred to as a "ping" - at the VA's Office of Information and Technology (OIT). However, I have spoken with several people from OIT and was informed there was no such "alarm" or notification when someone who does not have authorization accesses a C-file.

I have been trying for several months to obtain a list of every person who has ever accessed, viewed, and/or queried any part of my C-file. It is every veteran's right to know who has been viewing their private information. The VA promised me I would receive an unredacted audit. However, the list the VA sent me was incomplete. There were many missing names and dates. VBA claimed that those were all the people and dates that they could find. However, I have evidence proving otherwise. When I informed the VA, in October 2017, of the missing names and dates, I was told the VA would look further into it. I have not received anything to date from this October request. When I recently requested a status update on the audit of my C-file, I was told that VA FOIA requests were backlogged. I originally informed VA leadership in Washington DC of the privacy violation in early July 2017, as well as, requested an audit of my C-file at that time.

The person who is currently scrubbing the audit list of my C-file is the Director of the RACC, Ms. Kim Graves who totally disregarded my letter asking for RACC protection and assigned my C-file to the Oakland VARO, against my permission. When I asked OIT why they could not directly mail me the audit, I was informed that OIT "had" to send audits to the director of the regional office that has jurisdiction over my C-file. This absolutely makes no sense at all. Having the VA patrol itself is like having a fox guard the hen house. As you already know, Kim Graves has demonstrated her lack of integrity, so it is difficult to have confidence in her abilities. She and Diana Reubens are also tight with some of the Oakland VA regional office managers who are using the VA system to retaliate.

VA leadership has been informed that my former managers and co-workers at the Oakland VA Regional Office retaliated against me by trying to use my C-file against me. Yet nothing has been done about it, no one has been held accountable, no one has been prevented from accessing my C-file and hardly anyone returns my communication. I am having difficulty obtaining help from both VA employees, or the Veterans Service Organizations, not because they do not want to help me, but because, as they all put it, and quite frankly I have lost count on the number of people who have told me this, they are all afraid to help me for fear that they will be targeted like me; they are afraid of being "blacklisted" or "blackballed", they fear they will lose their job and/or VA benefits.

What does it say about our country when veterans are afraid to speak out against unethical and illegal practices at the VA for fear of retaliation? I have a lot of support in the shadows, but no one has been willing to step out into the light and be my champion, because it is seen as a fruitless mission; instead of creating meaningful change, the mission would be more like falling on one's sword. I am grateful to have found Whistleblowers of America because they understand whistleblower retaliation and are willing to give me a voice today.

We ask that Congress act on behalf of veterans so that they can obtain an accurate audit of a his/her C-file and to protect veterans' privacy. The solution to update VBA's security control system for digital C-files is to have Congress legislate new laws that can make VBA do so. The VA cannot be trusted to fix this security problem, because VA directives, memorandums, and protocols can be changed by the VA at any time, as well as, their interpretation and adherence to their own made up rules. A well written law minimizes ambiguity and ensures adherence and accountability.

I started a petition on Change.org, called "*Protect Jamie's Private Medical Info from Her Former VA employers and Make Them Accountable*," so I could get the attention of our legislatures. (I am represented by Representative Mike Thompson and Senator Kamala Harris who are aware of my situation.) I was told I would gain the ear of Congress if I could obtain at least 100,000 signatures. Although this petition has my name on it, protecting veterans' privacy is not just for me, but for every veteran

Every veteran has a right to know, in a timely manner, who has been viewing their private information and why. There must be an enforceable law to deter people from accessing a veteran's C-file without first having authorization or permission by the veteran. Congress can

pass a law that make each veteran a watchdog over their own C-file by releasing unredacted audits of their C-file immediately upon request and whenever requested. Audit logs could be readily accessed at any time via the eBenefits portal, which would show the veteran via live coverage, who is and has been viewing their protected information. Congress should pass a law that require the reporting of privacy violations to be made easy and efficient, as well as, hold VA managers and employees accountable for privacy violations. Congress should pass a law that make sure VBMS and any other VA computer system has functional and accurate audit logs that can accurately pinpoint security violations.

Thank you for your time and consideration.

Whistleblowers of America is a 501C3, EIN 82-3989539. Its mission is to provide peer support to employees and veterans who have reported wrongdoing and experienced retaliation.

Jamie Fox is a whistleblower from Oakland, CA who reported harassment of a co-worker and suffered retaliation while working in the Oakland Regional Office. She is currently employed at another VA facility. This statement is made on her own time and not representative of the VA.