



Photo by: David Law

US Department of Veterans Affairs:

Policy, Administration, and Healthcare concerning OIF and OEF (Operation Iraqi Freedom, Operation Enduring Freedom) Veterans.

David Law

4/11/2007

Public Administration - Prof. Mazurana

This subject was initiated through my Military Science 221 course. The final exam is to teach a class, 45 minutes in length, on a subject that has not been covered in lessons materials. While some Cadets thought of WWII history, internal policies/protocol, and unit specific interests; personally, there was a desire to really approach this as an opportunity for these young soldiers to learn something. Since four out of eight cadets have already completed at least one tour in Iraq, and one stationed in Afghanistan, their eventual discharge and status as Veterans came to mind. Through each generation, horror stories exist in soldiers' difficulties transitioning from their military experiences to civilian life. For this reason alone was the drive to call the US Department of Veterans Affairs for assistance in addressing this issue.

At first, the concept almost seemed intimidating, too grand and stifling. How would/could someone get their head around such a vast bureaucracy as the VA? To get a better understanding of the Human Services side, references to the VA's "Veterans Benefits Association" provided specific information on OIF and OEF administrative reform. With the increasing demand of performance, time commitment, and potential deadly situations involving US Armed Forces. The existing infrastructure of Veterans Affairs was woefully inadequate to meet the demands of agile, reactionary services needed in the 21st Century. New benefits package for all service members include: After initial discharge, access to VA Healthcare is granted for two years even without any service-connected illness. **1** Veterans with illness or injury always have access to VA Healthcare with no time limit. **1** Transition Liaisons for the severely wounded. **1** (Counselors and Rehabilitation Specialists)

Getting past the high-gloss marketing of “improved and better than ever” section; reasons behind the desperately needed reorganization began to surface. Of the most common WIA Not RTD (Wounded in Action, Not Returned to Duty) status soldiers, their injuries were Muscular/Skeletal Conditions and Hearing Disorders. Additionally, Amputation, Sensory Loss, and Brain Injury result from the devastating IEDs and RPGs (Improvised Explosive Devices and Rocket Propelled Grenade) attacks in Iraq and Afghanistan. **1** Despite such massive loss, these soldiers survive traumas, which in past wars would have proven fatal on the battlefield. In doing so, this exerts pressure for changes (admin/policy/routines) upon VA Medical Centers and how they fundamentally function. Poly-Trauma Centers are becoming the new necessity as brain injuries among received casualties become the “signature of the current conflict”. **1**

“...One early scientific study indicted the estimated risk for PTSD from service in Iraq was 18%. While the estimated risk of PTSD from the Afghanistan mission was 11%, data from multiple sources now indicate that approximately 10 –15% of soldiers develop PTSD after deployment to Iraq; and another 10% have significant symptoms of PTSD, depression, or anxiety and may benefit from care ...” (Pg 1) **1**

Seeing that dependency upon Veterans Affairs Rehabilitation Services is only likely to increase, the reliability of its infrastructure, in theory, should match in capability.

However on May 3, 2003, the burglary of a VA Analyst’s Maryland home resulted in the loss of his laptop -- with sensitive data for over 26.5 million veterans.

“...“Words are inadequate to describe how I feel about these recent events and the impact on the band of brothers and sisters of service members and veterans that we are supposed to serve,“...” **2**

Deputy Assistant Secretary. McLendon's resignation followed this statement, citing his responsibility to take action and serve as a proper example to staff and the Public.

According to Congressional testimony, the Public was notified on May 22nd. 19 days after the incident occurred. **2** Whether this was exercise of public disclosure, or an attempt to internally quarantine damage control, communications between policy and management were retarded severely.

"...Deputy Assistant Secretary. McLendon notified officials, then advised Deputy Secretary Gordon Mansfield, on May 10, no official action until the VA Inspector General heard about the data theft through office gossip the same day, beginning its own investigation..." **2**

Internally, the incident may seem as a direct failing of an individual charged with sensitive information to outside agency observers. Then becomes an issue of administrative policy and procedural enforcement failings across the board.

For instance, it remained a violation of policy for VA employees to take work home, but the Data Analyst had already been doing so for three years before the break-in occurred.

2 Surely the Analyst understood the risks of allowing personal data to leave facility jurisdiction and into the less secure environment. In fact, his notification of direct managers was almost immediate after the security breach. Citing scale of the loss in the laptop and its sensitive contents.

"...According to congressional testimony, the VA data analyst immediately told his supervisors -- including Mr. McLendon -- after the theft of a laptop and disks that contained veterans' birth dates, Social Security numbers and disability ratings at the data analyst's Aspen Hill home..." **2**

Again, the critical issue of responsibility seems to get lost within the very nature of bureaucracy itself. In the ability to either deflect and divert necessary steps for a secure and accountable governing body; the overwhelming temptation arises in just skipping over process and appointing a figurehead to take the organization's failing.

"...We can't be blaming this whole thing on some data analyst and his boss. There are many more individuals in this chain of command that I hope would be held accountable "

- Bob Wallace, Executive Director of Veterans of Foreign Wars..." **2**

Herein lies the real question within the obligation of liability and functioning as an agency now in charge of an increasingly reliant population of returning veterans. Not only does the compromised status of personal data undermine the goals of the department itself, the situation demoralizes current enlisted personnel that will be coming into the system in the future.

Commentary from Don Macvittie of Network Computing magazine, writes in his article:

"VA Admins: Hold Your Fire", that only punishing a motivated employee would send the wrong message to both the public and private workplaces regarding administrative accountability.

"...Average employees do not take work home with them; only motivated employees-an organization's best employees-do that. Firing this worker will send a message that will ripple through both the public and private sectors: "Take work home with you, and we will fire you." **3**

While motivation is essential in any field of work, it should not dismiss the need of security awareness or that relaxed or non-existent policies should be supplemented by what someone feels is the appropriate precautions/comfort level. Addressing this issue,

Francis Bueb examines in his piece: “Line of defense: simple, complex security measures help prevent lost and stolen laptops” from General Business File ASAP, signals that Certified Public Accountants are now responsible for much more than just bookkeeping. “...CPAs used to secure data in their offices or locked in briefcases. Today, however, with the ease of accessing and storing sensitive information on laptops, CPAs need to reconsider how they keep client information confidential and secure...” **4**

Bueb depicts the dilemma CPAs face in confronting the convenience of laptops as potential security risks to their client’s information and the contractor/firm. Taking common-sense security precautions, he says, will go a long way before having to think about compromised data. Always consider where the laptop is being taken, and if sensitive information is present, do not even put it on the laptop. Ensuring pen drives are not plugged into the laptop unattended, and basic measures as Cable Lock Kits be installed. **4** Briefings of regular security policies/employee roles in those duties is critical to maintain integrity and a more controlled defense plan. If confidential files are lost, to understand both the cost of recouping and deploying effective countermeasures to prevent further damage is needed.

These seem fairly practical, inexpensive, and easy solutions to aid in stemming the hemorrhaging crisis of network security failures. Sadly, continual reports as recent as April 5, 2007, USA Today revealed over 460 stolen or lost computers from Internal Revenue Service facilities since 2003.

“...The computers were lost in 387 incidents, most of which were not reported to the IRS computer security office as required, according to the report by the Treasury Inspector General for Tax Administration.

The audit also found that IRS laptops lacked adequate password controls and encryption software that would protect taxpayer information and other data...” 5

Although the consistent struggle with interagency security seemed to be localized in massive US Government SNAFU. In reality, it is a problem all entities encompassing both sectors (public and private) face in the new Digital Age. Such as, the loss of a hard drive in our own University of Northern Colorado campus, compromising the personal data of both faculty and students for possibly years to come. The human element will always remain in its own governance, and with it, the untold number of mistakes, disasters, and uncertainty of life that comes with it. There seems to be a culture of forgetfulness associated with the advent of technologies and the marvels they deliver. Before the loss of notebooks, books full of notes have always been stolen or lost. Absent was a sensationalized press release, or ever present “putting out fires” that managers confront daily. To play devil’s advocate, technology only serves to magnify the preexisting conditions to both new levels of benefits and exploitations. Identity theft is nothing new, but its proliferation rate and the underground industry it has turned into is. Perhaps as well, personal accountability has not caught up with the changing times, and a significant gap is exposed to create the criminals playground that exists.

After conducting the initial research, as a good Bureaucrat, Junior Grade; there was no way to present such a portrayed bleak picture to eight Cadets selflessly serving their country. An initial call to the Greeley VA Medical Center resulted in the referral to the Cheyenne VA Medical Center. Theresa Garduno, Supervisor of the facility, notified the Press Release division. Dan Frantz established contact, a 20 year Psychiatric Nurse at the VA Cheyenne Clinic. Additionally, Damion Dawes a Secretary to Supervisor

Garduno will also be presenting. The US Department of Veterans Affairs commitment and enthusiasm, to communicate directly with the Military Science class, is telling of the character in men and women whom will serve them as Veterans.

Both gentlemen are scheduled to appear on April 12, 2007. Discussion topics will include a general introduction to what the US Department of Veterans Affairs offers for veterans, new OIF and OEF benefits package from Damion Dawes. Dan will cover the advantages to Mental Healthcare services within VA Medical Center locations. The intent, is to put forward a human face and presence for often thought and stereotyped ambiguous government machinery. Just as the recent debacle with the Walter-Reed Medical Center outpatient facility, has produced even more of a negative image of the VA. There is a desperate need to show current service members that a support system is in place and will not abandon them during such trying times -- for military and public administration departments. Of things learned within this project, it is the efforts of those behind the front lines and armed forces that make the difference. In a roundabout way, it is bureaucracy that allows for such a complex and interconnected system to even function. Even for one as all encompassing as the US Department of Veteran Affairs.

Works Cited:

1. Fact Sheet: "VA Services for Returning Combat Veterans of Operation Iraqi Freedom and Operation Enduring Freedom"
November 2006 Edition
Department of Veterans Affairs

As in compliance with the Superintendent of Documents of The US Government Printing Office: This is a replication of original US Government documentation that may be found at:

Office of Public Affairs (80D)
810 Vermont Ave.
Washington, D.C. 20420

2. "VA Assistant Secretary steps down"
Washington Times Online
Associated Press
May 31, 2006.
URL: <http://www.noodletools.com/quickcite/citwww2.html>

3. **VA Admins: Hold Your Fire.(Veteran Affairs)(Brief article).** Don Macvittie.
Network Computing (June 8, 2006): p17. From *Computer Database*.

4. Line of defense: simple, complex security measures help prevent lost and stolen laptops.(PRACTICEMANAGEMENT). Francis Bueb.
California CPA 75.5 (Nov 2006): p27(3). From General Business File ASAP.

5. "Personal data at risk in lost IRS laptops"
McCoy, Kevin
USA Today
April 5, 2007
URL: http://www.usatoday.com/money/perfi/credit/2007-04-05-irs-usat_N.htm?csp=34