STATEMENT OF JERRY L. DAVIS
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATION,
HOUSE COMMITTEE ON VETERANS' AFFAIRS
June 4, 2013

INTRODUCTION

Chairman Coffman, Ranking Member Kirkpatrick and members of the Subcommittee, thank you for the opportunity to convey my concerns to you regarding the protection of information systems and information, which includes sensitive Veteran data at the Department of Veterans Affairs (VA).

From August 2010 until February 2013, I served as the Deputy Assistant Secretary, Information Security (DAS IS) and Chief Information Security Officer (CISO) at the VA. As the DAS, IS I served as the most senior civil service staff member within VA with responsibility for oversight and accountability in the protection of VA information, VA privacy, records management and the Freedom of Information Act (FOIA) process. At the time of my departure from VA in early February 2013, I was one, if not the longest serving Chief Information Security Officer (CISO) in the federal government with nearly a decade of service in that role spread across multiple federal agencies. I am also a Marine Veteran having served in combat with distinction during the First Gulf War, so the appointment to the position as the VA CISO had special meaning. It was a position that I did not take lightly and I was and I still am extremely proud to have had an opportunity to serve our country and equally proud to have had a great opportunity to serve the Veteran community.

My time at VA was largely filled with a great sense pride because of the purpose and mission of VA and because of my role, which had a direct and positive impact on the Veteran community. However there came a time at the end of my tenure where my pride turned to serious consternation and that consternation remains this very day.

SECURITY POSTURE IN 2010: VA's COPROMISED ENVIRONMENT

In nearly 20 years of building and managing security programs across government and private industry, I had never seen an organization with as many unattended IT security vulnerabilities. Upon my arrival in late August 2010 I inherited the results of more than 15 continuous years of an unattended and documented material weakness in IT security controls. This material weakness included more than 13,000 uncompleted IT security corrective actions. These 13,000 security corrective actions would require more than 100,000 sub actions to fully remediate and manage IT security vulnerabilities and improve the VA security posture. In early September 2010, I also was advised that nearly 600 VA systems' Authority to Operate (ATO) had expired and there was no plan in place to bring these systems into compliance.

Despite the voluminous number of uncompleted corrective actions and expired ATOs, the most concerning issue was the conversation I had with the VA Principle Deputy Assistant Secretary (PDAS), Stephen Warren, who told me shortly after my arrival that "We have uninvited visitors in the network". Further discussion with the VA Network Security Operations (NSOC) team indicated that VA became aware of a serious network compromise in March 2010 and these "uninvited visitors" were nation state-sponsored attackers. Over the course of time while working with the VA NSOC team and external agencies, I learned that these attackers were a nation-state sponsored cyber espionage unit and that no less than eight (8) different nation-state sponsored organizations had successfully compromised VA networks and data or were actively attacking VA networks; attacks that continue at VA to this very day. These groups of attackers were taking advantage of weak technical controls within the VA network. Lack of controls such as encryption on VA databases holding millions of sensitive records, web applications containing common exploitable vulnerabilities and weak authentication to sensitive systems contributed to the successful unchallenged and unfettered access and exploitation of VA systems and information by this specific group of attackers.

During my tenure, I consistently insured that each instance of attack or compromise by these group of attackers was documented and communicated to the VA OIT leadership through specialized reporting called Key Investigative Reporting (KIR) performed by the NSOC Deep Dive Analysis (DDA) team and biweekly security meetings with the VA Principle Deputy Assistant Secretary (PDAS), Mr. Stephan Warren.

MITIGATION ACTIVITIES 2010-2013

From late August 2010 until my departure in early February 2013, I planned for and executed with support from various sub offices within OIT a series of initiatives and activities needed to improve network and systems security with a particular focus on defending the network against sophisticated and targeted attacks levied by nation-state sponsor organizations. Some of these initiatives included the Web Applications Security Program (WASP), the VA Software Assurance Program, Continuous Monitoring and Diagnostics (CMD) of VA information systems, and mandating encryption of VA databases, and supported the reduction of the total number of VA databases hosting sensitive Veteran information.

During my tenure as CISO, with the support of VA as a whole, we were able to close more than 10,000 of the 13,000 security corrective actions. In all, VA personnel executed more than 100,000 sub actions. While these actions did improve security from a compliance perspective, there still existed a problem of fully implementing adequate technical security controls needed to defend networks, systems and sensitive information from nation-state sponsored attackers. The heart of selecting the proper technical controls meant fully understanding the threat actors, their tactics, techniques and procedures (TTPs) and along with system and network vulnerabilities and implementing a program that could continuously report on and remediate identified vulnerabilities in a near real time fashion.

Over time, the Office of Information Security (OIS) worked to enhance a comprehensive program called Continuous Monitoring and Diagnostics (CMD) that would provide adequate security of VA systems and networks by continually evaluating certain technical controls in a near real time fashion. There is proof that a good CMD program monitoring the correct controls can significantly improve information security and is consistent with the direction that the federal government has taken in securing federal systems. It is also significantly superior to even a good paper based ATO process.

OIT LEADERSHIP DEVIATES FROM ATO PROCESS

It is my testimony that at the time of my departure from VA that the processes required for the DAS, IS to make an attestation that VA systems were adequately secure was completely faulty and improper and the implementation of the process exposed Veteran systems and VA information to further risk of compromise. It was confirmed to me by the VA information security staff charged with executing the process that it was flawed, provided no value and that a providing a positive attestation to the adequately of security controls would seriously compromised the integrity of the VA security program. I subsequently conveyed this message to the Assistant Secretary and the PDAS by formal memorandum and in conversation to the PDAS between January 15, 2013 and January 23, 2013.

VA Handbook 6500.3 states that the DAS, IPRM (now called DAS,IS) is responsible for:

(3) Reviewing all C&A packages and making a decision recommendation to the AO to issue an IATO, ATO or <u>Denial of Authorization [emphasis added]</u> to operate; and
(4) Providing an IATO extension in the event local management can demonstrate continuous monitoring and security due diligence are being provided….

In accordance with VA information security policy and following VA information security procedures, As the DAS, IS, I elected to recommend a denial of an authority to operate and also elected to recommend movement of VA systems over the course of eight (8) months into an enhanced continuous monitoring program, where systems technical controls could be centrally managed and evaluated in a near real time fashion. I based my decision on the guidance provided by the information security team and on the fact that the paper based process would not keep highly sophisticated nation-state sponsored attackers from further compromising VA data. Furthermore, as each VA system was transitioned into the continuous monitoring program, additional specific critical controls would be evaluated for adequacy before being granted a full ATO. These additional critical controls are proven to slow and repel sophisticated, nation-state sponsored attackers from compromising information systems and data. This was an agreed upon process with the VA information security team and a process that had been briefed by me to the Director of IT Audits and Security within the VA Office of the Inspector General (OIG) several weeks before the process implementation.

Despite the authority granted to the DAS, IS to make a recommendation to deny authorization, the VA OIT PDAS made a concerted effort to circumvent my authority and influence my decision to make a recommendation to the Accrediting Official (AO) that 545 VA systems be given an IATO. Furthermore, VA handbook 6500.3 and VA policy 6500, provides for no role or authority for the PDAS, OIT with regard the program or processes governing Authority to Operate.

RECOMMENDATIONS

To this end, I would recommend that this subcommittee:

1. Review all VA Key Investigative Reports (KIRs) and Deep Dive Analysis (DDA) reports and Web Application Security Program reports (WASP) to assess the damage and depth of exposure, extent of compromise to VA systems and compromise of Veteran information; and
2. Regularly report to the House Committee on Veteran Affairs on progress made with respect to mitigating access to VA systems and Veteran information by nation-state sponsored organizations;
3. Assess previously identified web application exposures and assess for potential compromise of Veteran data, both PII and PHI;
4. Include web application exposures as part of the Data Breach Core Team (DBCT) evaluation process;
5. Assess the potential compromise to non VA networks sharing an interconnection with VA's network;
6. Designate the VA network as a "compromised environment" and establish controls that are effective and support the reclamation of control back to VA from nation-state sponsored organizations;
7. Move the VA systems into a full continuous monitoring and diagnostics program with near real time situational awareness of its security posture with a focus on the 20 critical controls;
8. Increase VA funding for information security programs; and number of Information Security Officers (ISOs) supporting VA field offices and facilities
9. Move reporting lines for the DAS, IS directly to the AS, OIT or to the Office of the Secretary, VA
10. Assess the past and present practices of the OIT leadership with regard to decisions made in the protection of VA systems and information.

I would like to thank the members of the subcommittee for your time today and I look forward to any questions you may have.