Statement for the Record of
Bruce A. Brody, CISSP, CISM
Vice President, Information Security, INPUT
Before the
Committee on Veterans Affairs
U.S. House of Representatives

June 22, 2006

Mr. Chairman, Ranking Member Evans, and Members of the Committee. My name is Bruce Brody. As a veteran, I am very thankful for the opportunity to address this distinguished Committee today.

I am the Vice President for Information Security at INPUT, a market research firm based in Reston, Virginia. From 2001 to 2004, I was the Associate Deputy Assistant Secretary for Cyber and Information Security at the Department of Veterans Affairs, and from 2004 until January of this year, I was the Associate Chief Information Officer for Cyber Security at the Department of Energy. I believe I am the only person ever to have served as the Chief Information Security Officer (CISO) at two Cabinet-level Departments.

During the period from 2003 until my retirement from federal service early this year, I served as a member of the Information Security and Privacy Advisory Board, created by Section 304 of the Federal Information Security Management Act of 2002, to advise the National Institute of Standards and Technology, the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to federal information systems. In that capacity, I gained very broad insight into the information security and privacy practices of many federal agencies. I would also note that my federal service was interrupted by a three-year stint in private industry where I gained a lasting appreciation for the practical application of risk management principles in dealing with security and privacy issues.

My position at INPUT affords me the opportunity to provide neutral analysis and insights to nearly 1,200 corporations concerning information security developments in the federal government. I do not work for any federal customers. In recent months, I have also been approached for dozens of interviews to the media concerning the flaws of

the Federal Information Security Management Act (FISMA), the challenges of implementing Homeland Security Presidential Directive 12 (HSPD 12) and the loss of private information that was in the custody of the Departments of Veterans Affairs and Energy. I am hopeful that I can provide this Committee with some background, details and personal perspectives to assist in bringing this unfortunate incident to some degree of resolution.

In my summary remarks, I provide an overview of my experiences with the Department of Veterans Affairs that form the basis for several recommended corrective actions for this Committee to consider. I realize that not all of these corrective actions are within the purview of this Committee, but I am confident that your colleagues in other committees will realize the need to act.

Like members of this Committee and my fellow veterans, I view the loss of the personal information of more than 26 million veterans as willful disregard for responsible behavior and blatant contempt for established federal security and privacy requirements by senior VA leadership. While I doubt that my personal information was compromised in the recently-disclosed loss of information from the Department of Energy, I empathize with the hundreds of individuals holding security clearances who are only now learning that their personal information was compromised.

I urge this Committee to look carefully at the following factors, which I believe contribute to the decades of information security and privacy neglect at the Department of Veterans Affairs that have been documented by the Inspector General and the Government Accountability Office.

First and foremost, someone with the appropriate substantive expertise has to be empowered to set and enforce privacy and cyber security requirements, to include the physical security requirements for how such records are maintained and the personnel security requirements for whom access to such records is allowed. It is my recommendation that this Committee legislate the requirement for someone to function in the private sector role of a Chief Security Officer, possibly with the title Undersecretary for Risk Management.

The responsibilities of the Chief Security Officer would be to directly advise the Secretary concerning information, physical and personnel security, privacy, and other risks to VA information, facilities, resources and the veterans whose interests VA must protect. The position must be equal in stature with the Administration Undersecretaries and, under the supervision of the Secretary and with congressional oversight, would promulgate security and privacy policies across the Department, enforce accountability for compliance, oversee implementation of remediation strategies for removing identified shortfalls and coordinate the Department's budget related to these issues.

When I was first introduced to this Committee as the new VA CISO in April 2001, I thought that the Secretary had hired me for the purpose of implementing effective cyber security controls. However, I learned over time that the apparent authorities invested in the CIO in the Clinger Cohen Act and the Paperwork Reduction Act, and in the CISO in Computer Security Act of 1987, the Government Information Security Reform Act of 2000 and finally in FISMA, were not accepted by VA or its leadership.

I quickly learned that the Department's Chief Information Officer (CIO) only had authority to "advise, encourage, support and persuade" the Administrations insofar as information technology programs were concerned. In addition, I learned that the CIO had no authority to "direct" compliance with – at that time – the Paperwork Reduction Act. These points were captured in a memorandum from the Assistant General Counsel dated October 6, 2000.

Difficulties with this "advise, encourage, support and persuade" approach to the CIO's management authority were raised at a March 12, 2002 Oversight Committee hearing by both Chairman Buyer and Ranking Member Carson who questioned the ability of the then-CIO to get the job done without "line authority." Later that year, Secretary Principi took actions to direct the centralization and enhanced line authority of the CIO function, presumably acting at least in part on the recommendations of this Committee. Unfortunately, the Secretary's direction met with bureaucratic inertia and cultural resistance and was never fully implemented.

For many decades, the culture of the VA has been one that enables and promotes fierce resistance to change, stiff opposition to central authority and active refusal to adopt

best security practices. In my three and a half years at the VA, I faced these chronic issues on a continuous basis. Whenever a security initiative was introduced, it was common practice for the Administrations and Program Offices to resist, impede and obstruct the initiative both to prevent any diminution of local authority and to interfere with anything other than business as usual.

Subsequent to my arrival at the VA, the Government Information Security Reform Act (GISRA), followed by the Federal Information Security Management Act (FISMA) were enacted in 2000 and 2002, respectively. Not being an attorney, I cannot offer legal opinions about what the words of those statutes mean. I can only apply common sense to the purpose of these important pieces of legislation. It seemed to me that if, after all was said and done, the opinion of the Assistant General Counsel issued in October of 2000 was correct, then the Congress went to nonsensical amounts of effort to produce the legislation and provide such details concerning specific responsibilities.

It became all the more apparent that clarification was needed following the MS Blaster malicious software incident in the second half of 2003.

In advance of what proved to be the serious malicious software attack represented by MS Blaster, my office provided the necessary alerts, and also distributed notification concerning the necessary patches throughout the VA enterprise. These alerts were widely ignored, and VA networks were savaged as a result. The ensuing recriminations included a review by a medical doctor in the Veterans Health Administration (VHA) who was supposedly renowned for conducting root cause analyses. His analysis of this incident concluded that the CIO's Office was at fault for not convincing the Administrations and the Program Offices that we were really serious when we told them to install the required patches to mitigate the attack.

Thereafter, the Office of Inspector General became heavily involved in criticizing the absence of common security controls as well as the recommended configuration control board structure of NIST Special Publication 800-40. The OIG mistakenly pointed at the Office of the CIO as the responsible office for those deficiencies.

From my perspective, these negative accusations did not compute. The apparent authorities invested in the CIO in the Clinger Cohen Act and in the CIO and CISO in

FISMA did not seem to be accepted by VA or its leadership. As a result, I concluded that there was no longer any point in attempting to introduce cyber security changes in VA unless there was a clear statement of authority to do so. That was when I requested the General Counsel opinion about FISMA authorities for the CIO/CISO.

Just prior to the MS Blaster attack, I had requested a clarification from the General Counsel concerning the responsibilities of the CIO under FISMA for national security and non-national security information and information systems. In a memorandum signed by the General Counsel on August 1, 2003, it was reinforced that the various security functions of the Department, specifically information security, physical security and personnel security, would remain under the authority of their respective offices. According to the memorandum, the CIO was allowed to issue policies pertaining to information security, but the daily operations of security clearance determinations, investigations, physical storage and related activities were not to be placed under the purview of the CIO.

Subsequent to the MS Blaster attack, I requested a clarification from the General Counsel concerning the authority of the CIO to enforce compliance with security legislation and regulations. In a memorandum signed by the General Counsel on April 7, 2004, it was asserted that the CIO cannot order or enforce compliance with information security requirements. Because FISMA used the word “ensure” instead of “enforce” the General Counsel stated that the only recourse for the CIO when a security requirement was violated was to complain to the Secretary.

The result of these two opinions was extremely unfortunate for the Department. In effect, the first of these memos fragmented security authorities and the second said that the CIO had no authority to enforce policies or hold people accountable for violating policies. These memos accurately captured and reinforced the culture of the Department, where resistance to central authority and maintaining the historical ‘norm’ of doing business according to hundreds of different local practices have always been the practice. In day to day operations, these memos ensured that the fragmentation of security authorities enabled the lack of background investigations for individuals with access to VA networks, systems and resources; the unchecked access to VA information by foreign corporations and foreign nationals; limited to non-existent logical and physical access

controls for major medical systems; the disruption and denial of service from malicious software attacks such as MS Blaster in 2003; and hundreds of other negative information security findings as highlighted in the reports of the independent public auditor, Inspector General and Government Accountability Office.

I would ask the Committee if it agrees that the Clinger Cohen Act and FISMA do not require the Secretary, CIO and CISO to set and enforce the security requirements of the FISMA legislation. I would also ask the Committee if it agrees with the opinions of the VA General Counsel.

If you accept the legal opinion of the VA General Counsel, then the Secretary, Deputy Secretary and Undersecretaries are the only officials who had the authority to implement and enforce the policies, procedures, accountability and culture that would have prevented the loss of the 26 million records that bring us together today. I would be quite surprised if that position regarding responsibility for information security oversight was part of the Secretary's in-briefing to the Department.

If, as I suspect, the Committee does not agree with the VA General Counsel, then corrective action must follow. If FISMA and the Clinger Cohen Act do not convey the authority and accountability for enforcing security and privacy requirements, perhaps the Congress needs to amend these bills to so state. My personal experience is that the mismatch of authority and accountability for the CIO and CISO affects other departments and agencies to the same extent that it affects the VA, and I encourage legislative action to clarify this situation and possibly prevent more serious incidents from occurring.

But the bottom line for the VA was that the two General Counsel memos reinforced the VA culture, and the VA culture is the root cause of this problem. The VA culture can be highlighted even further in the paper trail of non-concurrences on VA Directive 6500, Information Security Program.

My second recommendation is that policies, procedures and assignments of accountability regarding security and privacy issues cannot be held hostage to the individual interests of the senior officials whose concurrence must be obtained prior to review by the Secretary. In this regard, I invite the Committee's attention to the paper trail of non-concurrence on Draft VA Directive 6500, Information Security Program.

Draft VA Directive 6500 represented the effort of my office to modernize a 1999 VA information security and privacy policy. Following extensive discussions with the Office of Inspector General and GAO auditors, VA Directive 6500 was intended to put in place the necessary policy to reduce security vulnerabilities; remove the causes of negative IG, GAO and independent auditor findings, including the information security "material weakness"; comply with all FISMA and Privacy Act security and privacy requirements; and establish a means for enforcing accountability for non-compliance with the policy.

The MS Blaster experience and VA Directive 6500 drafts are the quintessential VA examples of the lack of accountability and the culture of obstructionism. The concurrence process for VA Directive 6500 became a frustrating, albeit illuminating, exercise in forcing the Administrations to put into writing their individual positions on information security fragmentation and the CIO's authority. The Committee's attention is invited to this paper trail in order to witness first-hand the culture of resistance that is at the heart of the current incident.

On January 16, 2004, VHA non-concurred on VA Directive 6500, disagreeing with a blanket approach to background investigations, opposing any requirement to ensure that corporations having access to VA systems and data be American-owned – in other words, subject to U.S. laws and within the reach of U.S. courts if U.S. laws were breached. VHA also opposed any requirement that visitor personnel be escorted at VA facilities and resisted the ability of the ADAS for Cyber and Information Security to establish mandatory penalties for non-compliance. On January 23, 2004, the Acting Assistant Secretary for Policy, Planning and Preparedness non-concurred with the Directive, providing the ill-informed statement that information does not lend itself to the oversight and management of one organizational entity, and further emphasizing the need to keep fragmented the security disciplines of cyber security, information security, information management, physical security, enforcement authority, continuity of operations and personnel suitability and security. On February 19, 2004, the General Counsel non-concurred on the Directive because it failed to clarify the "limited" role of the CIO, and it reiterated that the CIO could only "ensure" and not "enforce" compliance.

The General Counsel further instructed that language be removed that pertained to the CIO holding people accountable for non-compliance.

The memos by the General Counsel and the paper trail of non-concurrence on VA Directive 6500 are indicative of a culture of resistance to central authority and refusal to accept anything other than business as usual. They also highlight the decentralized authority enjoyed by the Administrations and Program Offices, who are empowered to define the role and authority of the CIO as they see fit in order to perpetuate their parochial interests. Most of all, these documents make it clear that the CIO and the subordinate CISO have no authority to do anything other than issue policies, but on top of that, they can only issue policies that the Administrations and Program Offices allow them to issue through the concurrence process. Once issued, the CIO and CISO have no authority to enforce the watered-down policies that they are permitted to put into place.

As a third recommendation, let me suggest to you that the CIO budget, including cyber security and privacy budgets, cannot be held hostage by the Administrations and Program Offices. Since funds are not directly appropriated to the CIO by the Congress, security and privacy initiatives depend on the funding support of the very offices that have historically been the cause of the problems being addressed.

During the Fiscal 2004 budget year, the Administrations held hostage the budget of the Office of Cyber and Information Security subject to a review by low-level field personnel who, in some instances, were significant violators of cyber security practices. Final funding release was not granted until late June 2004, leaving only the final Fiscal Year quarter to execute a substantial portion of the entire year's budget.

Fourth, I recommend you create a legislative requirement that would suspend all executive and senior bonuses in the VA until the environment for which the executive is responsible receives a clean bill of security health from the IG and the competent senior official placed in charge of security. Here again, the Committee will find an illuminating paper trail concerning the efforts of OCIS to implement mandatory Senior Executive Service performance appraisal criteria, which, although approved by the Secretary, could not be effectively enforced.

Fifth and finally, the Committee needs to look very closely at the workforce mix in the critical area of privacy, cyber and information security controls. The Committee has been dealing with issues pertaining to the culture of the VA on numerous occasions over the past decade. It is truly unfortunate that it takes another crisis to highlight the continuing need for culture change at the VA. I am not optimistic that the VA culture will change, nor am I optimistic that this incident will be the last of its kind at the VA.

There are more than 26 million veterans and active duty personnel who are uncertain if the loss of their personal information will bring them financial harm. These veterans deserve better, because they have served our country well. Unfortunately, the VA has not served them well, and the VA must make the necessary amends. If the VA cannot reinvent itself and change its culture dramatically, then I would beg the Congress to do it for them, and to do it for our nation's deserving veterans.

Toward that end, I note that it has been the policy of the VA over the past few years to replace contractor staff with full time VA employees. Since cyber and information security is a very dynamic field of expertise where static approaches will inevitably be overwhelmed by rapid advances in attack methodology, regular technology enhancements are essential. The agility, training and expertise to implement these new technologies will be difficult to achieve with a workforce governed by federal personnel processes and regulations.

As a veteran, my heart goes out to our war wounded, those who have sacrificed so much to keep us free and safe. I would encourage this Committee to develop programs that help those war-wounded to transition into such highly specialized high technology occupations.

Mr. Chairman, that concludes my statement. Thank you for the opportunity to appear before you today.