STATEMENT OF
THE HONORABLE ROBERT T. HOWARD,
ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY,
DEPARTMENT OF VETERANS AFFAIRS,
BEFORE THE SUBCOMMITTEE
ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY
U.S. SENATE

MARCH 12, 2008

Good Afternoon Chairman Carper and members of the Subcommittee. Thank you for your invitation to discuss the ability of the Department of Veterans Affairs (VA) to protect and secure sensitive data. Information protection is a top priority within VA and is highlighted as one of the five principal priorities in the FY06-11 VA Strategic Plan. As you are aware, May 3, 2006, was the day of the theft which led to the temporary loss of personally identifiable information (PII) of up to 17.5 million veterans, some of their spouses and some active duty personnel. Although our investigation confirmed that the PII was never accessed, that day was a wake up call, not only for VA, but for the entire federal government as well as the private sector. As a result of that incident, we began to improve our security posture and create the environment needed to better protect the sensitive personal information of veterans and VA employees-as well as any sensitive information entrusted to us. Today, I would like to briefly share with you some of these initiatives.

Clearly, the centralization of Information and Information Technology (IT) within VA has had a positive impact regarding the protection of sensitive information. Within this new structure we have established a separate organization called "Information Protection

and Risk Management (IPRM)" that is dedicated to improving our overall data security posture. A new Deputy Assistant Secretary (DAS) position has been established to lead this organization and help provide the important focus that is needed.

IPRM is thoroughly examining every aspect of our information protection posture in the areas of cyber security, privacy, records management, incident response, field security and business continuity to ensure that sensitive protected information (SPI), primarily PII, and Protected Health Information is not compromised. The goal is to protect the integrity, authenticity and confidentiality of VA's SPI. In essence, VA is committed to ensuring that its data is protected from unauthorized access, modification, destruction, disclosure or disposal while at the same time making it readily available for those who are authorized to use it.

Several key leaders from this organization are here with me today, Adair Martinez, my DAS for IPRM, Jaren Doherty our new Chief Information Security Officer (CISO) who is also in charge of Cyber Security, Kathryn Maginnis who is in charge of Incident Response and Risk Management, Sally Wallace who leads our efforts in the area of Privacy and Records Management, Charlie Gephart our Director of Field Security Operations and Andy Lopez who has recently established our office of Business Continuity. In addition, Arnie Claudio – the Executive Director for the Office of IT Oversight and Compliance (ITOC) - is also here today. These individuals form the VA leadership core for information protection and are focused on the implementation of a

wide variety of activities that are moving us to a much more secure posture than that which currently exists within VA.

One of the most important steps we have taken to help create a robust information security environment is to develop a comprehensive action plan, called the *Data Security - Assessment and Strengthening of Controls* program (DS-ASC). It focuses on three major areas: 1. Managerial--for example the establishment of policies and directives, 2. Technical--for example better software tools and equipment such as encrypted thumb drives, and 3. Operations--examples here would be the establishment of procedures to provide an enhanced employee training environment and overarching programs to enhance individual employees' awareness of their information security responsibilities. The DS-ASC program, which includes several hundred specific actions, is oriented on improving the position of VA in the entire area of information protection. To date, about 40 percent of the actions have been completed.

One especially important action was the completion and publication of VA Handbook 6500, dated September 18, 2007. This handbook describes the VA Information Security program. It contains the primary cyber security procedural and operational requirements Department-wide to ensure compliance with the Federal Information Security Management Act of 2002 (FISMA) and the Information Security provisions of title 38 of the US Code as well as provide for the security of VA information and information systems administered by VA, or on behalf of VA. It also includes the National Rules of

Behavior – a document that employees must sign before they are given access to our computer systems and sensitive information.

Standardized information protection policies, processes and procedures are clearly established in VA Directive and Handbook 6500. These are being implemented, and we are making progress in creating an environment of vigilance and awareness regarding individual responsibility in the area of information protection - an extremely important aspect of our overall program.

While we have made progress, there is still much to be done. With respect to FISMA, there are five problematic areas: Annual Testing and System Inventory; the Plan of Action and Milestones (POA&M) process; Certification & Accreditation of IT Systems; Configuration Management; and Security Awareness Training. I will address our progress in each of these areas.

Annual Testing and System Inventory – During FY07 100 percent of VA's IT systems underwent testing to include testing of contingency plans. We have also recently initiated efforts to improve the FISMA inventory to better characterize contractor-controlled systems.

POA&M Process – We are prioritizing POA&Ms and producing daily reports on the status of remediation actions. We are also tracking all IG-reported deficiencies in our

SMART database so that those deficiencies are accounted for in the total number of POA&Ms reported to OMB.

Certification & Accreditation (C&A) of IT Systems – Based on IG recommendations and an independent verification and validation study, VA has taken an aggressive approach in redesigning the C&A process. An intensive effort is underway to complete this work by the end of FY 08, when we have to certify and accredit (C&A) over 600 IT systems in accordance with FISMA. We have also developed a new process for FY09 and beyond where we will C&A 1/3 of all IT systems each year. Continuous monitoring and control testing will be accomplished by the team that has been established for the ongoing C&A efforts. This team involves all segments of the organization, to include a permanent C&A office as well as regional points of contact for C&A work. I am confident that our FISMA performance in this area will improve as a result of our new C&A processes.

Security and Privacy Awareness Training – Over 90 percent of all VA employees have received security and privacy awareness training. We are also using the Learning Management System (LMS) provided by OPM's HR Line of Business (LOB). This will provide for better tracking of all VA employee and contractor training. By improving the tracking, we believe we will be able to improve the accuracy of our reporting and increase the percentage of all VA employees and contractors who receive security awareness training. This system should be implemented Department-wide by the end of fiscal year 2008.

The improvements in these five areas, coupled with the recent appointment of an experienced CISO, should favorably impact our FISMA performance in FY 2008.

We have also recently transferred our Field Security organization to our DAS for Information Protection and Risk Management. This realignment will further strengthen security support to field organizations and provide all regions direct linkage for implementing information protection strategy, policies, processes and procedures throughout VA. This change meets one of GAO's recommendations.

Our incident response program is another area that has been substantially improved A well organized process is now in place wherein incident notifications received from the field that report possible exposure of sensitive information, including veteran or VA employee PII, are quickly processed, to include simultaneous notification to the U.S. Computer Emergency Response Team (US-CERT). In each case where a veteran's or VA employee's PII could be compromised, notification is sent to them with an offer for credit monitoring and/or credit protection services. In response to Public Law 109-461, Title 9 of the Veterans Benefits, Healthcare and Information Technology Act of 2006, we are also using the GSA Blanket Purchase Agreement (BPA) for independent risk analysis. We have definitely established a very robust and aggressive process for dealing with incidents. These procedures are prescribed in the Directive/ Handbook 6500 and in VA's incident response Standard Operating Procedures (SOP). We would prefer not having any incidents to process, but at least we are now able to deal with them.

We also have made substantial improvements in the area of internal assessments. These assessments focus on compliance with Directive and Handbook 6500. The ITOC was established a year ago. Using a very comprehensive checklist, this organization has already completed over 200 assessments and is having a positive impact across VA. The ITOC assessment program of 24 to 30 assessments per month is far more aggressive than the two per month experienced in the past. ITOC is working Department-wide to correct and help eliminate existing deficiencies found by the Inspector General and the General Accounting Office over the last few years. ITOC is also helping to effect real change to improve VA's FISMA compliance efforts, and continues to work with each VA Administration and Staff Office to mentor, train, and coach in order to promote an environment where the sensitive information entrusted to us is better protected.

Even with all we have accomplished, we still experience security and privacy incidents. Except for a few, these incidents usually involve the sensitive personal information on a small number of individuals. We consider any data breach to be serious if veteran or employee sensitive personal information is at risk. Many of these incidents are the result of human error and carelessness, which is why it is so important to establish a culture and a strong environment of awareness and individual responsibility. The training and education of our workforce is probably the single most important action on our list. While it may be impossible to predict, let alone prevent every security or privacy incident, it is the primary goal of VA's information protection program.

In closing, we have a variety of aggressive programs in place that will ultimately help us achieve the 'Gold Standard' in data security which, since the summer of 2006, has been a major goal of the Department of Veterans Affairs. Much more remains to be done, but I remain personally committed to working toward achieving this *Gold Standard* goal and can assure you that VA senior leaders are equally committed. We all recognize the need to establish a world class security environment wherein we can fully safeguard the sensitive and private information of veterans and employees-and all sensitive information entrusted to us. Thank you for your time and attention today – I'm prepared to answer any questions you may have.