STATEMENT OF
THE HONORABLE TIM S. MCCLAIN
GENERAL COUNSEL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
JUNE 22, 2006

Mr. Chairman and Members of the Committee,

I am pleased to be here this morning to discuss certain legal implications of the May 3, 2006, theft from a VA employee's home of personal-identifying information concerning veterans, service members and some spouses.

As you are aware, three class-action lawsuits have been filed alleging that the Department has violated the Privacy Act and the Administrative Procedure Act in the theft of these records. Two of the lawsuits name as defendants, in their individual capacities, the Secretary, the Deputy Secretary and the employee from whose home the records were stolen. The lawsuits seek amounts that could total billions of dollars from the United States because of this theft. Because of those pending lawsuits, it would be inappropriate for me to discuss how the relevant laws apply to the facts giving rise to those suits.

Legal Aspects of the Data Loss

The Privacy Act applies to individually-identified records, such as those stolen on May 3, about individuals that the Agency retrieves by the names of those individuals, regardless of the storage media used to maintain the records. The BIRLS database involved in the VA data loss is an example of an electronic, Privacy Act-protected set of records.

The Federal Information Security Management Act (FISMA) applies to Federal information and information systems, including systems operated by VA contractors.

Both the Privacy Act and the Federal Information Security Management Act provide a framework for establishing agency safeguards to ensure the security and confidentiality of records. These statutes generally outline agency responsibilities and do not address the duties and responsibilities of individual Government employees except as to the willful and intentional disclosure of Privacy Act-protected information.

The HIPAA (Health Information Portability and Accountability Act) Privacy and Security Rules do not apply to the stolen data. Within VA, only the Veterans Health Administration is an entity covered by the HIPAA Privacy and Security

Rules. The data involved in the loss all either came from Department of Defense personnel records or were created by VBA as part of its claim adjudication process. It is our opinion that these are not activities covered by the HIPAA Privacy Rule.

Legal Aspects of Federal Information Security Management

Under the Federal Information Security Management Act (FISMA), the Secretary must provide protection from "unauthorized access, use, disclosure, disruption, modification or destruction" of VA information and information systems by:

(1) complying with information security standards required by law, the Office of Management and Budget (OMB), and, as to national security information and information systems, the President;
(2) requiring VA "senior agency officials" to provide security for their information and information systems, in accordance with the FISMA-mandated risk analysis process;
(3) creating, through the Chief Information Officer (CIO) and senior agency information security officer (ISO), an agency-wide information security program, conformance with which shall ensure that the information security standards are met and the risk analyses are performed;
(4) providing for sufficient personnel trained in information security requirements; and
(5) requiring annual reports from the CIO "in coordination with other senior agency officials."

FISMA requires the Secretary to delegate to the CIO sufficient authority to "ensure compliance" by the agency with the above information-security requirements. This must include the authority to (1) create and operate the agency-wide information security program; (2) establish information security policies and procedures and control techniques for the agency, which, when followed, will ensure compliance with all of the above requirements; (3) train and oversee personnel with significant responsibilities for information security; and (4) assist senior agency officials concerning their information security responsibilities, including the analysis process.

The agency-wide security program directed by FISMA should provide systematic guidance for the conduct of the risk analysis process, security awareness training for all VA personnel, periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, a process for remedial action, procedures for detecting security incidents, and plans for ensuring continuity of operations for information systems. The policies and procedures should interpret, explain, and apply to VA the applicable external standards and provide guidance for the application of these standards to VA

operations. The control techniques should permit monitoring of the numerous activities in which programs are required to engage to determine that they are accomplished in accordance with applicable standards and that any appropriate remedial actions are timely undertaken. The program, policies, procedures, and control techniques, and any other actions, should be developed in mutual coordination, cooperation, and collaboration between the CIO and program officials.

FISMA does not prescribe the means for the CIOs' "ensuring compliance." The legislative history indicates that, by establishing the senior ISO, Congress intended to implement the GAO-observed information-security best practice of establishing a "central management focal point to ensure adequate attention to information security." That does not necessarily require delegation to the CIO of direct control over agency programs, because such control is not the only means by which the information security-objectives may be accomplished. For example, even without direct control over certain programs, a CIO could endeavor to ensure compliance with governing standards through training and otherwise influencing the behaviors of key program-security personnel. While an agency head certainly may choose to confer certain enforcement powers on the CIO, e.g., the ability to sanction program officials outside the CIO's immediate organization for noncompliance with departmental policies, we do not read FISMA to require it.

Ultimately, an agency head is responsible for the agency's compliance with FISMA. If he or she determines the agency is otherwise able to operate in full compliance with FISMA's information-security requirements, he or she need not provide the CIO with enforcement powers. In that circumstance, the CIO's recourse for perceived non-compliance would be to exercise the prerogative of directly reporting to the agency head, which is mandated by the Paperwork Reduction Act of 1995 (44 U.S.C §3506(a)(2)(A)).

Mr. Chairman, at the Committee's June 14, 2006 hearing, you took issue with an April 7, 2004 opinion issued by my office to two VA Assistant Secretaries (including the CIO) regarding the extent of the authority granted by FISMA to the CIO. This opinion followed an earlier (August 1, 2003) opinion of my office, and I have attached copies of both opinions to this statement. Consistent with our understanding of the Act, we advised in those opinions that:

- FISMA clearly contemplates that Department officials will comply with the information-security program, policies and procedures developed by the CIO, receive assistance and training from that office regarding these responsibilities, and cooperate with the information-security techniques of that office;

- However, FISMA places upon the Secretary the responsibility for ensuring agency compliance with its provisions, and leaves to his

discretion how to do so. The Secretary could, if he chose, delegate to the CIO various enforcement powers.

We also stated specifically in the April 4 opinion that in a March 16, 2004 memorandum to departmental officials, then-Secretary Principi had tasked the CIO with devising and developing a Department-wide cyber-security program under FISMA, and had directed cooperation in the implementation of those policies as they were developed. In this memorandum, the Secretary also announced his "intention" to imbue the CIO with all power and authority needed to carry out his responsibilities for cyber security, to "include certain administrative and supervisory authority over employees directly involved in the implementation of cyber security policy under appropriate directives, policies and personnel regulations" which the Secretary indicated "[were then] being drafted to effectuate my intentions."

We indicated in our April 7, 2004 opinion that the Secretary's memorandum signaled his intention to delegate enforcement powers to the CIO that, we anticipated, would be specified in the written directives he signaled would be forthcoming. We understand you, however, to be of the view that the Secretary's March 16, 2004 memorandum itself constituted a delegation to the CIO of any and all enforcement authority deemed necessary to ensure security-policy compliance throughout the Department.

It may be helpful to briefly state what the Department has done to implement Secretary Principi's 2004 memorandum. In an October 19, 2005, memorandum, Secretary Nicholson ordered the reorganization of VA's IT operations. In February 2006, the Secretary advised senior Agency officials at a senior management retreat that VA's IT reorganization was his top priority. In that regard, on April 30, 2006, approximately 4,000 FTE were temporarily detailed to the Office of Information and Technology (OIT) as part of the implementation of the October 19 memorandum. As of the end of the current fiscal year, those employees will be permanently transferred to OIT. At that point, all IT operations and maintenance will be centralized in OIT. As you know, the VA Chief Information Security Officer is in OIT, which recently issued VA Directive 6504 establishing mandatory security requirements for all VA information systems.

Mr. Chairman, I would add that, similar to FISMA, neither the Paperwork Reduction Act nor the Clinger-Cohen Act of 1996, which also prescribe duties of the CIO, imbue the CIO with specific enforcement powers over employees of other elements of an agency.

Thank you, Mr. Chairman, for the opportunity to testify on these very important issues.