STATEMENT OF
PETER S. GAYTAN, DIRECTOR,
VETERANS AFFAIRS AND REHABILITATION COMMISSION
THE AMERICAN LEGION
BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
ON THE
DRAFT LEGISLATION TO BETTER PROTECT THE SENSITIVE PERSONAL INFORMATION OF VETERANS

JULY 18, 2006

Mr. Chairman and Members of the Committee:

Thank you for this opportunity to present The American Legion's views on this proposed legislation. On May 3, 2006, the home of a Department of Veterans Affairs (VA) employee was burglarized. The burglary was reported to the local police. It is reported that the employee discovered that computer equipment, which contained personal information on approximately 26 million veterans and military personnel, was among the items stolen, he immediately notified VA management in the Office of Policy, Planning, and Preparedness, including Security and Law Enforcement personnel. The employee reportedly advised all of them that the stolen personal computer equipment contained VA data. However, the VA Secretary was not informed of the incident until May 16, 2006, almost 2 weeks after the data was stolen. The Congress and veterans were not notified until May 22, 2006. VA's failure of leadership in establishing Information Technology (IT) reform over the past three years has undeniably led to the current crisis we are now addressing.

While the stolen laptop and external hard drive have been recovered and reports from the F.B.I. stated that the information on the equipment was not accessed, The American Legion's position is that legislation still needs to be enacted to protect all effected veterans and servicemen from any possible future unauthorized release of their personal information. Even a high likelihood that the information was not accessed is not a guarantee that it was not. According to the July 11, 2006 report of the Office of Inspector General (OIG) there was no, "encrypting or password protecting the data." Originally, VA tried to mitigate the risk involved saying that most of the critical data was stored in files protected by a statistical software program, making it difficult to access. The OIG reported that, "This, however, was not the case because we were able to display and print portions of the formatted data without using the software program."

Equally disturbing is the more recent news of other security breaches that have only come to light because of the spotlight that is now on the VA. It wasn't until a follow up hearing on the data breach on June 29, 2006 that 10 pages of security breaches were presented to this Committee to include an incident in Minnesota that occurred in 2005. The August 1, 2005 cut off date in the proposed legislation puts veterans who may have had their information compromised before that time at risk of having no help from VA in the future. Because we may

never know the extent of the lapses in VA IT security, it is The American Legion's position that VA be appropriated the necessary funding to monitor all veterans' credit who are victims of identity theft as a result of security breaches regardless of when these breaches may have occurred. On June 21, 2006, Secretary Nicholson announced that the VA would provide one year of free credit monitoring to people whose sensitive personal information might have been stolen in the latest incident. This promise should not be broken. The Secretary stated, "Free credit monitoring will help safeguard those who may be affected, and will provide them with the peace of mind they deserve." The American Legion agrees with the Secretary's statement.

The American Legion is supportive of the proposed legislation and the attitude of Secretary James Nicholson which are in agreement with what the VA OIG report recommended, namely: (1) take whatever administrative action deemed appropriate concerning the individuals involved; (2) establish one clear, concise VA policy on safeguarding protected information when stored or not stored on VA automated systems; (3) modify mandatory Cyber Security and Privacy Awareness training; (4) ensure that all position descriptions are evaluated and have proper sensitivity level designations, and that required background investigations are completed in a timely manner; (5) establish VA-wide policy for contracts that ensures contractors are held to the same standards as VA employees and that protected information used on non-VA automated systems is safeguarded; and (6) establish VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems.

The American Legion also offers the following recommendations related to the draft legislation:

Section 4. Department of Veterans Affairs Information Security: Under **section 5721. Definitions,** subparagraph (7), which identifies what sensitive personal information is, should include any information with regard to family members as well.

Under section 5725. Provision of credit protection services and fraud resolution services: This section does not address the issues of whether or not the victim will be liable for any fiscal loss due to VA's mistake; to what extent the VA will make the victim whole; how are multiple occurrences of identification theft handled?

Under subparagraph **(g) (2) Fraud Alerts,** what happens if identity theft occurs after the one-year monitoring period? What if stolen data is held for longer than one year before it is used?

Finally, The American Legion wants legislative assurances made to veterans that if their information is compromised by VA, unless it is undeniably the result of some other cause, the VA or federal government will assume the responsibility of any loss incurred by the veteran or relevant family members. Veterans should never be required to have to prove it was the fault of VA that they were the victims of identity theft if VA has already put them at risk.

The American Legion urges patience in allowing the Federal government to continue working toward a fair and expeditious resolution to this matter. It is the position of The American Legion that to bring the judicial branch into this by filing a lawsuit will only impede the process. Filing a lawsuit against the VA will not act as a catalyst for reform; in fact, it will slow down the

process. Neither will it expedite the passing of legislation that would compensate veterans for the cost of monitoring and protecting their current credit ratings and personal accounts or for those who may become victims of identity theft.

The American Legion stresses the importance of a swift resolution to this issue by avoiding the inevitable delays and unfair rulings that often result from class action suits. The outcome of the Agent Orange class action settlement should serve as a reminder that judicial oversight isn't always the best remedy. This historic case did not equate to fair compensation for veterans exposed to Agent Orange. Out of about 105,000 claims received, 52,000 totally disabled veterans or their survivors received payments averaging approximately $3,800. This certainly didn't cover the health care for these severely disabled veterans. However, the lawyers who split the $9.2 million granted by in attorney fees weren't complaining.

The data theft that occurred in May has served as a monumental "wake up call" to the nation. VA is no longer ignoring IT security. The American Legion is hopeful that this legislation along with the steps VA takes to enhance and enforce its IT security will renew the confidence and trust of veterans who depend on VA for the benefits they have earned. We reiterate the point that funding for the IT overhaul should not be paid for with money from other VA programs. This would in essence make veterans pay for VA's mistakes. The American Legion urges that VA and Congress will not attempt to fix this problem on the backs of America's veterans.
In addition to a fair and expeditious resolution to this breach of security at VA, there should be a complete review of IT security government-wide. VA isn't the only agency within the government that needs to overhaul its IT security protocol. The American Legion urges the President and Congress to review each Federal agency to ensure that the personal information of all Americans is secure.

Mr. Chairman, The American Legion appreciates this opportunity to express its views on this legislation and the issues surrounding it. We look forward to working with you and the members of the committee to make sure comprehensive changes take place in the VA regarding the security of sensitive personal information to the benefit of veterans, active-duty service members, Reservists and their families.

This concludes my testimony.