Statement of the Honorable
Gordon H. Mansfield
Deputy Secretary
Department of Veterans Affairs
Before the Committee on Veterans' Affairs
U.S. House of Representatives
July 18, 2006

Mr. Chairman and Members of the Committee,

I am pleased to provide the Department's views on eight bills, all intended to protect the personal privacy of veterans and others affected by the May 3, 2006 theft of computer equipment containing veterans' personal data. While you had also invited our views on a draft bill your staff shared last week, I regret that time has not permitted us have cleared positions on its many provisions. We will supply those for the record once the necessary executive-branch coordination is completed.

Initially, I wish to point out that the eight bills covered in my testimony were introduced before the stolen computer hardware was recovered. As you know, the FBI has concluded with a high degree of confidence that, based upon its forensic examination and other evidence developed during its investigation, the veterans data were not accessed or compromised prior to their recovery. That development has eliminated the need for much of what is proposed in the legislation, and while we understand the concerns that engendered these eight bills we do not support their enactment.

H.R. 5455

H. R. 5455, the "Veterans Identity Protection Act of 2006," would require the Department of Veterans Affairs to: (1) provide notification to each individual whose personal information was included in the recent data breach; (2) provide to any of these individuals a free one-year credit monitoring service; (3) provide a copy of that individual's credit report once annually during the two year period following the termination of the credit monitoring services; and (4) certify in writing to Congress that any individual whose personal information has been compromised due to data security lapses at the Department has been appropriately notified in writing

The Secretary has already taken proactive and aggressive steps to notify all individuals whose personal information was potentially at risk as a result of the May 3 data theft. Also, the recovery of the data, apparently uncompromised, eliminates the need to offer credit monitoring or additional free credit reports at this time**.**

In addition, the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq*., requires each of the three major credit bureaus to provide, upon request, a free copy of an individual's credit report once every twelve months and upon the individual's placement of an initial fraud alert on his or her credit file. Therefore, an individual who places an initial fraud alert could make a request to each of the three credit bureaus and receive up to six free credit reports annually. The Department's website at http://www.va.gov. documents the actions taken by the Secretary in this regard and advises veterans how to place a fraud alert with, and obtain free credit reports from, the credit bureaus. For these reasons, H.R. 5455 is unnecessary.

H.R. 5464

H. R. 5464, the "Veterans Identity Protection Act," would require VA to: (1) provide detailed notification to each veteran whose personal information was included in the data breach; and (2) include a form for the veteran to elect to receive a free credit report once every three months for the year following notification and free credit monitoring for that year also. The bill also would limit the funds available to Office of the Secretary to 90 percent of the funds otherwise available if the 16 information security recommendations of VA's Inspector General are not fully implemented by January 1, 2007. The bill would limit the funds otherwise available to the Office of the Secretary by 10 percent in subsequent fiscal years, after January 1, 2007, for any information security recommendation not fully implemented.

VA supports the underlying intent of H.R. 5464, but cannot support the bill. In addition to the actions already discussed, VA is taking steps to implement the 16 information security recommendations. The Secretary has established an Information Security Task Force composed of senior officials and has hired a Special Advisor on Information Security. Working together with the Chief Information Officer of the Department, these individuals will implement the recommendations. For these reasons, we believe that H.R. 5464 too is unnecessary.

H.R. 5467

H. R. 5467, the "Veterans Identity Security Act of 2006," would establish criminal penalties for knowingly disclosing without authorization records containing personal information about veterans. The bill would amend title 38, United States Code, by adding a new section 5706 applicable to officers, employees, contractors, and volunteers of the Department who disclose personal information without lawful authorization. The bill defines personal information as "name, date of birth, address, phone number, Social Security number, and (if applicable) disability rating." Penalties range from fines to imprisonment for up ten years when there is intent to sell, transfer, or use the personal information for commercial advantage, personal gain or malicious harm.

VA has no objection to the intent of H.R. 5467 but has several technical suggestions for improving its drafting and coverage. We would be happy to discuss these with Committee staff at its convenience.

H.R. 5487

H. R. 5487, the "Veterans' ID Theft Protection Act of 2006," would also require VA to notify any person affected by the breach, but also to notify consumer reporting agencies and appropriate third parties who may be required to act in a manner to further protect affected persons from fraud or identity theft. The notice specifications must include details of the breach, current safeguards of personal information, contact information for the Department, information provided by the Federal Trade Commission (FTC) regarding identity theft, information on obtaining a copy of a consumer's credit report free of charge and other information regarding placing a fraud alert on one's file and contact information for the FTC. The bill also would require the Department to offer affected persons free credit monitoring service, at their request, for not less than six months, and to take prompt and reasonable measures to repair the data breach that would improve the data security policies and procedures.

For reasons already discussed, H.R. 5487 is unnecessary.

H.R. 5490

H. R. 5490, the "Veterans Identification Protection Act," would require the Department of Veterans Affairs to: (1) provide a four-digit personal identification number (PIN) for each veteran who receives or applies for VA benefits, and (2) take steps to provide that any entity entering into a commercial transaction with a veteran that "includes the extension to the veteran of credit, a loan, or any other thing of value" shall verify the veteran's identity through the PIN established. Any entity that is required to so verify a veteran's identity, but fails to, would be liable to that individual for all attorney fees and injuries incurred by that individual resulting from that failure.

VA does not support H.R. 5490. VA understands that the current level of security as recommended by the National Institute of Standards and Technology and other security experts requires a PIN number with more than four digits. However, even if the bill were amended in this regard, VA would be opposed to the requirement that the Secretary provide, assign, monitor, or validate any universal PIN number exclusively for the use of veterans in commercial enterprises. The bill is unclear about the commercial enterprises to be covered. For example, there is no distinction made between commercial activities with a VA involvement (such as a home loan guarantee) and other commercial activities a veteran may be involved with that have no VA connection.

H.R. 5577

H. R. 5577, the "Veterans Identity Protection Act of 2006," is intended to enhance the protection from disclosure of VA records containing personal identifying information that is required by law to be confidential and privileged.

It would require the Department to establish an Office of Identity Protection, administered by a Director who shall be appointed by the Secretary. The Office would notify each individual whose personal information has been lost or compromised, provide him or her with one credit report every six months for three years at no charge, offer a 24-hour toll-free telephone number and a web site to provide information regarding credit reporting services, ensure that active-duty military personnel have access to credit reporting services, make information available on possible fraudulent consumer credit or reporting services that may be targeted at affected veterans and service members and notify the Department of Justice and the FTC immediately when personal data in VA records may have been compromised. Furthermore, the Act would require the VA Inspector General (IG) to conduct a study of the data-security practices at VA and submit a report not later than six months after the date of the law's enactment to the Senate and House Committees on Veterans' Affairs. Finally the Act would impose criminal penalties of a fine or imprisonment on any VA employee who removes records from VA custody without proper authorization.

VA supports the underlying purposes of H.R. 5577, but cannot support the bill. In addition to the ameliorative actions already discussed, VA has provided a toll-free telephone number and a section on the Department's web site with information for those individuals seeking assistance, and established an Information Security Task Force to improve data security. While the Information Security Task Force will consider administrative alignments to enhance data security protections, there does not appear to be a need for a separate administrative Office of Identity Protection at this time. And, as already noted, FCRA already provides up to three free credit reports annually, and up to another three annually when an initial fraud alert is placed. For these reasons, we do not believe that these provisions are necessary.

The requirement for the VA IG to report on the Department's progress in implementing data security improvements within six months after the law's enactment would not allow sufficient time for the Department to address corrective actions before the report must be submitted. Furthermore, the VA Inspector General regularly issues reports about data security practices within VA in Federal Information Security Management Act (FISMA) audits and consolidated financial statement audits performed annually. There does not appear to be a need for additional reports in this area.

In addition, the criminal penalty provision is not sufficiently specific for enforcement purposes. In particular, the bill does not specify whether "remove from the custody of VA," refers to removal from the "custody of a VA employee" or any removal from a "VA worksite." H.R. 5577 also does not consider the reality that files leave the worksite every day for legitimate purposes, nor does it identify the specific part of title 18 that would provide for the fines imposed for such action. We could support enactment of the additional criminal penalties in H.R. 5467 if those provisions were amended as discussed above.

H.R. 5588

H. R. 5588, the "Comprehensive Veterans' Data Protection and Identity Theft Prevention Act of 2006," would require the Secretary of Veterans Affairs to: (1) issue policies and procedures to safeguard sensitive personal information before the end of the 90-day period beginning on the date of the enactment of the Act; (2) notify the Secret Service, VA IG, Senate and House Committees on Veterans' Affairs, the FTC, and the affected individual of any breach: (3) place fraud alerts or security freezes in the credit file of affected individuals; (4) provide affected individuals with credit monitoring services; and (5) establish the position of an Ombudsman for Data Security within the Department to provide information and assistance to such individuals.

In light of the ameliorative actions outlined above, VA does not believe that H.R. 5588 is necessary and does not support enactment.

H.R. 5636

H. R. 5636, the "Social Security Numbers Privacy and Protection Act," would require: (1) the alteration of selective service reminder mailback cards; and (2), the elimination and prohibition of social security account numbers from Medicare, Medicaid, and SCHIP- and VA-issued health care identification cards by the end of the two-year period after the enactment of the Act

VA supports alternative methods for the identification of veterans for the purpose of providing health care or other benefits available under Title 38. To that end, VA has already removed the social security numbers from the Veterans Identification Cards known as VIC cards and is therefore already in compliance with the bill. With respect to Medicare, Medicaid, and SCHIP programs, the Department of Health and Human Services advises us that instituting a new number for use on the identity cards used for these programs would entail substantial expense and require a substantially longer time than allowed by the bill. They are continuing to work on these efforts. Therefore, we believe that enactment of H.R. 5636 would not be productive.

Conclusion

As I have indicated, VA already has implemented many of the provisions of the various bills that provide, among other things, stronger safeguards to protect against data breaches within the Department. VA is strongly committed to providing all available protections to the safety and security of personal information of all veterans' and their beneficiaries. As we continue to work on improvements in our systems and procedures, we will be pleased to work with your Committee in fostering methods to achieve a level of information security that is responsible and necessary.