Statement of Rep. Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
Hearing on the Security of Personal Information at Federal Agencies
June 8, 2006

Mr. Chairman, I am pleased that you are holding this hearing on federal data security.

Last month, sensitive data on 26.5 million veterans and active duty members of the military was stolen from the Department of Veterans Affairs. The Administration needs to provide the public with a thorough accounting regarding the VA incident. And it must detail how it will ensure that no future breaches occur with respect to the tremendous volume of information the VA and other federal agencies maintain on Americans across the country.

The recent VA data breach represents a violation of trust of remarkable magnitude. The Administration's failure to protect against such an incident – and its delayed response – may have made millions of men and women who currently serve and have served in uniform vulnerable to identity theft and other potentially costly misuse of their information.

Unfortunately, this breach does not come as a surprise.

Consider, for example, GAO's July 2005 assessment of information security in the federal government. GAO stated:

> Pervasive weaknesses … threaten the integrity, confidentiality, and availability of federal information and information systems. … These weaknesses exist primarily because agencies have not yet fully implemented strong information security management programs. These weaknesses put federal operations and assets at risk of fraud, misuse, and destruction. In addition, they place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

Indeed, in March of this year, in its annual scorecard evaluating agency information security practices, this Committee gave the federal government a governmentwide grade of D+. The VA received a grade of F.

Regrettably, the Bush Administration has repeatedly shown questionable commitment to protecting the privacy of American citizens. For example, last December, we learned that the President has authorized warrantless eavesdropping on Americans' e-mails and phone calls, despite federal laws forbidding this practice. Just this week, the *Washington Post* reported that since the federal medical privacy requirements went into effect in 2003, the Administration has received nearly 20,000 complaints alleging violations but "has not imposed a single civil fine and has prosecuted just two criminal cases."

I hope that the Administration will view the VA data breach as impetus for placing higher priority on privacy issues relating to the sensitive data it collects and maintains on Americans. As technological advances facilitate the sharing of information and as we develop new ways to use data on individuals to further important goals such as terrorism prevention, we must be vigilant about protecting Americans' privacy rights.

In the short term, the government must do everything possible to address expeditiously any harm resulting to the individuals whose data was stolen. The VA Secretary has taken several steps to provide information to veterans about the breach. But the Administration should be doing more to support the affected veterans and active service members.

I recently joined Rep. Salazar and over 100 other colleagues in urging President Bush to request emergency funding for free credit monitoring and additional free credit reports for veterans and others whose information was compromised. For our part, Congress should consider measures such as the Veterans Identity Protection Act of 2006, which Rep. Salazar has introduced. This bill would require the Department of Veterans Affairs to certify that it has notified all affected individuals. It would also direct the VA to provide free credit monitoring services and reports to each affected individual.

We must also determine exactly what went wrong at the VA to prevent future breaches. Toward that end, there is an ongoing joint investigation by the Inspector General, the Department of Justice, and local law enforcement, and I hope that today's hearing will advance our understanding of this issue.

Finally, the VA data breach should underscore the importance of ensuring implementation of sound information security practices governmentwide. The reports from the Office of Management and Budget and the Government Accountability Office show that some

agencies are making progress on this front. The A+ grade this Committee gave the Social Security Administration this year underscores that large agencies with aging systems and vast amounts of sensitive data can comply with federal information security requirements.

I want to thank the witnesses for taking the time to appear before the Committee today, and I look forward to hearing from them about the issues raised by the VA data breach.