OPENING STATEMENT OF
SENATOR FRED THOMPSON
CHAIRMAN
GOVERNMENTAL AFFAIRS COMMITTEE

March 2, 2000

Cyber Attack: Is the Government Safe?

Today, the Committee on Governmental Affairs is holding a hearing on the ability of the Federal government to protect against and respond to potential cyber attacks. This Committee spent considerable time during the last Congress examining the state of Federal government information systems. Numerous Governmental Affairs Committee hearings and General Accounting Office reports uncovered and identified systemic failures of government information systems which highlighted our nation's vulnerability to computer attacks -- from international and domestic terrorists to crime rings to everyday hackers.

We directed GAO to study computer security vulnerabilities at several Federal agencies including the Internal Revenue Service, the State Department, the Federal Aviation Administration, the Social Security Administration, and the Department of Veterans' Affairs. From these and other numerous reports, we learned that our nation's underlying information infrastructure is riddled with vulnerabilities which represent severe security flaws and risks to our national security, public safety and personal privacy.

Every year, the government gathers information on every one of us because we give the government this information in order to obtain government services – like getting social security benefits, veterans benefits, Medicare, or paying taxes. And yet, year after year, this Committee continues to receive reports detailing security breaches at these same agencies. Sometimes things improve – agencies usually will respond to specific GAO recommendations or to an particular Inspector General report. But, this is a "band-aid" approach to protecting information systems – fixing the system little by little, problem by problem, after it is revealed that it is no longer secure.

What is most alarming to me is that after all this time, and all these reports, there is still no organization-wide approach to preventing cyber attacks. And the security program management is totally inadequate. I'm afraid it's another example of how difficult it is to get the Federal bureaucracy to move, even in an area as important as this.

The reports highlight that an underlying cause of Federal information security vulnerabilities is inadequate security program planning and management. When GAO studied the management practices of eight organizations known for their superior security programs, GAO found that these organizations managed information security through continuous management activities which included specific practices to support their information security principles. We think this is lacking in the Federal government.

And we think agencies must do more than establish programs and set management goals – agencies and the people responsible for information systems in those agencies must be held accountable for their actions. And I believe that Congress should examine how we can provide assistance to the agencies to ensure that they have the resources necessary to maintain information technology security preparedness at all times.

It is clear to me, based on GAO report after GAO report, that what needs to emerge in government is a coordinated and comprehensive management approach to protecting information which incorporates the efforts already underway and takes advantage of the extended amount of evidence that we have gathered over the years. The objective of such an approach should be to encourage agency improvement efforts and measure their effectiveness through an appropriate level of oversight.

In order to develop such an approach and begin to find solutions to the problems which have been identified, we concluded that a more complete and meaningful statutory foundation for improvement is needed. That is why Senator Lieberman and I introduced S. 1993, the Government Information Security Act, at the end of last year. The primary objective of our bill is to address the management challenges associated with operating in the current interdependent computing environment.

Our bill begins where the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996 left off. These laws, and the Computer Security Act of 1987, provide the basic framework for managing information security. We view the introduced bill as just the beginning and recognize that these aren't the only things that need to be done. Some have suggested we provide specific standards in the legislation. Others have recommended we establish a new position of a National Chief Information Officer or even a national security "czar."

These issues and more will be brought up during our hearing today. The witnesses before us represent a broad array of experience and expertise in the area of information security. First, we have Mr. Kevin Mitnick who has described himself as a reformed hacker. Next, we will hear from Mr. Jack Brock who is the director of Governmentwide and Defense Information Systems at GAO and Ms. Roberta Gross, the Inspector General for NASA. Both of them have done significant work in the area of government information security. We also will hear from Mr. Ken Watson who is the manager of Critical Infrastructure Protection at Cisco Systems and Mr. James Adams, the CEO and co-founder of iDefense. I welcome all of you and look forward to your testimony about the cyber threats that we face today and how we can work together to fashion solutions to the many problems associated with computer security.