STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
FIGHTING THE PLAGUE OF WORMS AND VIRUSES

SEPTEMBER 10, 2003

Thank you Mr. Chairman for calling this hearing, and my thanks to the witnesses who have taken the time to be with us today and share their expertise.

Computer bugs like worms and viruses are on more example of the complexity of the world we live in. On the other hand, they are one more example of the frailty of human beings and the difficulty of legislating appropriate behavior.

Many of worms and viruses we have seen are nothing more than the exuberance of youth experimenting with newly found freedom and skills. As has always been the case, the pranks of youth can have consequences well beyond their capability to understand those consequences.

Last week, the FBI arrested a Minnesota high school senior and charged him with intentionally causing and attempting to cause damage to computers protected under federal law. He faces a $250,000 fine and up to 10 years in prison. This young man was so naive that he built into his computer bug a direct link back to his own computer. Catching him was not difficult. However, the damage done was real. The worm attack he participated in forced shutdowns of computer systems at the Federal Reserve Bank of Atlanta, the Maryland Motor Vehicle

Administration, the Minnesota Department of Transportation and part of 3M facilities, including a plant in Hutchinson.

Unfortunately, most hackers are neither as naive as this Minnesota teenager nor as benign. One of the earliest publicly documented cases of hacking was in 1988 at the Lawrence Berkeley Lab. Cliff Stoll, an astronomer turned systems manager at Lawrence Berkeley Lab, was alerted to the presence of an unauthorized user on his system by a 75-cent accounting error. His investigations eventually uncovered a spy ring that was breaking into government computers stealing sensitive military information.

We are faced with developing public policy that recognizes both the exuberance of youth, and the real threat to our government and corporations by those who seek to do us harm. One element of that public policy must be a renewed attention to preventing these attacks.

Earlier this year, several corporations were forced to shut down operations by a worm that took advantage of a known vulnerability in the Microsoft server software. Those who had installed the patch were unaffected. Those that had not were in big trouble.

For the federal government, there are two critical actions needed to solve this problem. First, we need sustained management attention to the day-to-day routine activities of computer security. Patch management is, perhaps, one of the least glamorous jobs in computer security. However, it is one of the most critical tasks. When something like the Slammer virus

from last January hits, government managers should reward those individuals who did their job and protected the agency systems. Second, the government needs to work with industry to assure that software with fewer holes is delivered, and that those holes that do exist are fixed as quickly as possible.

Let me take a few minutes to elaborate on this idea. The government has a large market presence in computer software. Recently, OMB has suggested that the government use that leverage to lower the cost of software. I believe a better use of that leverage would be to assure safer software.

Today, the price competition in the software market, has pushed profit margins to the point where investing in safer software may well be a life and death decision for a small company. The government, however, can use its purchasing power to encourage manufacturers to put on the market a more secure product. If a system manager can choose between a product that has been extensively tested for weaknesses and one that has not, in most cases the manager will choose the safer software, even if it costs more.

The second market innovation the government can promote is an ongoing relationship between the vendor and the customer. We see that today in the home market for computer security. Vendors of virus software offer services where the software is updated regularly for protection against new viruses. There is no reason that a similar relation cannot be forged between government purchases and all computer software. We need to encourage software vendors to be in the business of continually improving software security without forcing the user to purchase

and install a new version of the software. We also must create a market where security is profitable for software companies.

Our subcommittee chairman has indicated that he is working on legislation that would encourage corporate America to do a better job of securing their computers. I look forward to working with him on that legislation. The problems faced by corporations are much like those facing the federal government. We should work together to solve those problems.