Congresswoman Candice S. Miller

Opening Statement
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census
September 10, 2003

OPENING STATEMENT

Thank you, Mr. Chairman. I appreciate you holding this hearing today. With the recent computer virus attacks on our nation's information infrastructure, the importance of this hearing is undeniable and its timing is definitely appropriate.

With three panels testifying before us today, I will keep my comments short so that the witnesses can proceed with their statements. I look forward to each of your statements.

The focus of today's hearing is to examine what steps are being taken to protect the information infrastructure at both the public and private levels from the spread of viruses. We in the Federal government have the responsibility of protecting our citizenry and ensuring that the infrastructure individuals and businesses rely on is secure. In addition, the government must protect its own systems in order to function efficiently and effectively. This dual responsibility makes the task facing the Federal government particularly challenging.

In April of this year, testimony submitted by Robert Dacey of the GAO to this subcommittee cited a November 2002 cyber attack that affected both private and government networks and caused $900,000 in damage to computers. This is a significant figure; and if a large-scale cyber-attack were implemented, not only would the damage caused to computers be considerable, but the additional financial losses and damage to the physical infrastructure could seriously affect the operations of our nation.

We in the House of Representatives have first-hand knowledge of how potentially devastating these viruses can be. The recent Blaster and SoBig virus attacks of a few weeks ago nearly crippled the House email network by overloading servers with a complex array of erroneous messages. Fortunately, the combined efforts of House Information Resources and the systems

administrators in Members' offices limited the extent of damage that the viruses' creators had likely hoped for. In fact, these attacks likely inhibited our nation's ability to adequately respond to the vast power outage experienced by the eastern half of the country. I shudder at the thought of what could happen to everyday business if a successful virus or worm crippled our nation's power grids, financial networks, internet, government networks or any other infrastructure which we rely on so heavily.

Viruses are a new weapon of attack for those who wish to do harm to this great nation. The creators of these weapons are terrorists – plain and simple. Cyber-terrorists want to disrupt our way of life and to cause considerable harm to our economy and infrastructure. As with the terrorists we are fighting with conventional means, these cyber-terrorists are using the freedoms we hold dear against us. They can unleash an attack on our soil from anywhere in the world, and we must be prepared.

Mr. Chairman, thank you for holding this all-important hearing and I look forward to the testimony today. Protecting our nation's information infrastructure must be a top priority, and I hope the witnesses will add extensive insight as to do so.

Thank you.